Upstream Link for High-bandwidth Digital Content Protection

Revision 1.00

March 01, 2001

Notice

Intellectual Property

Implementation of this specification requires a license.

Contact Information

Email: info@digital-cp.com.

Revision History

15 June 2000	- 0.85 Revision. Initial publication at Copy Protection Technical Working Group
7 July 2000	- 0.86 Revision. Clarification of status bits, Authentication Context, Pipe ID Removal
16 August 2000	- 0.88 Revision. Clarification of Connection State, status bits; updated readZ; test vectors
21 August 2000	- 0.90 Revision. Miscellaneous clarifications and corrections (readStatus, Table 5-4)
12 October 2000	- 0.94 Revision. Clarifications in Section 5; updated test vectors; Table 8-1
18 October 2000	- 0.95 Revision. Add status bit 15; removed "Recommended Register Set" subsection
11 January 2001	- 0.96 Revision. Expanded definition of bits of Connection State
26 January 2001	- 1.00 Revision. No changes.

ISBN 0-9675129-8-0

1. Introduction

The High-bandwidth Digital Content Protection[1] (HDCP) technology requires adherence to the HDCP License's[2] compliance and robustness rules. These rules ensure that HDCP implementations both protect the confidentiality of keys and other values from compromise as well as deliver the desired protection for high-value video content. To meet these requirements, the HDCP Upstream Protocol has been developed to facilitate the implementation of HDCP on Personal Computers and other open platforms. On these platforms, the HDCP source device functionality is typically performed by a combination of the graphics hardware and video source application/middleware.

Figure 1-1 illustrates the relationship between the source application/middleware, the graphics driver, the graphics hardware, and the video receiver.

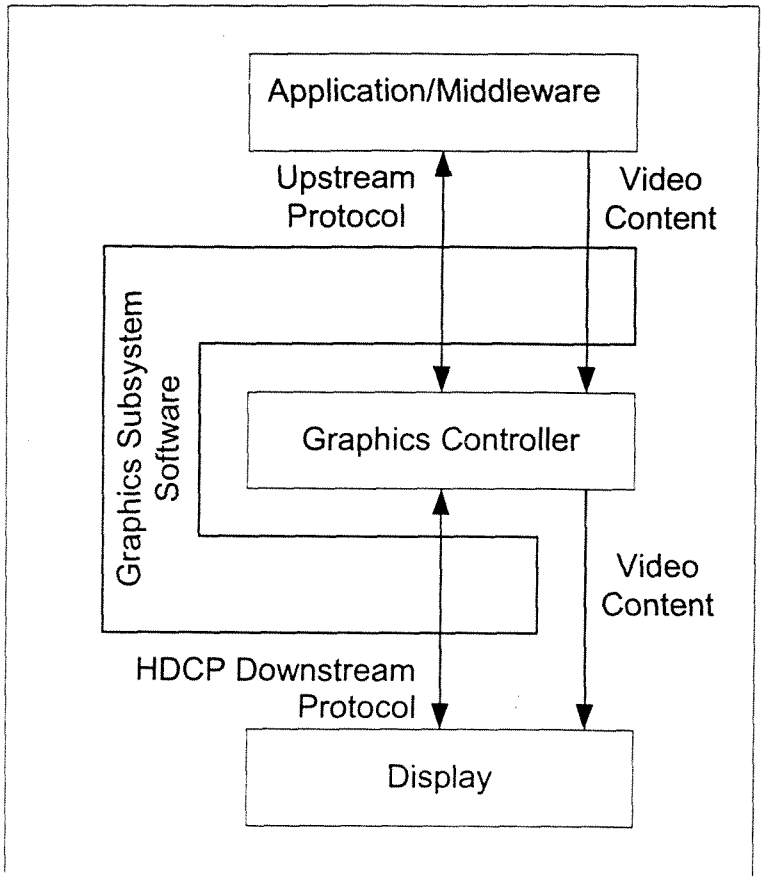

Figure 1-1. Upstream and Downstream Protocols

The Upstream Protocol is defined to allow the graphics subsystem software to facilitate both the Upstream and HDCP Downstream Protocols without handling confidential values, thereby avoiding the requirement of a tamper resistant component in the driver stack. Implementations of the Upstream

[1] High-bandwidth Digital Content Protection, Version 1.0, Intel Corporation, February 17, 2000.
[2] Available from www.digital-cp.com.

Protocol must meet the robustness and compliance rules specified in the HDCP Upstream Protocol Adopter License.

At system reset and hot plug events, the graphics driver facilitates downstream authentication between the transmitter hardware and the receiver hardware. For systems supporting HDCP, data will be encrypted between the graphics subsystem and monitor prior to the time that source applications load. Once loaded, it is the responsibility of source applications to determine the status of the HDCP protected link using the Upstream Protocol and to determine whether to deliver content through the video system based on that status.

2. Upstream Protocol

The Upstream Protocol is a cryptographic exchange between software and graphics hardware. The protocol requires a set of cryptographic keys for each protocol endpoint. Each set of 40 56-bit keys is the same size as that found in the HDCP protocol (the *downstream* protocol) for authentication between the DVI transmitter and receiver. The key agreement protocol between the endpoints begins with a key sum operation as in HDCP, allowing for reuse of graphics hardware necessary for the downstream protocol.

One difference between HDCP and the Upstream Protocol is that the Upstream Protocol establishes a key that is used to protect no more than 64 bits of data. Since very little ciphertext is revealed for each authentication, a relatively uncomplicated cipher may be used. The Upstream Protocol provides a mechanism for the encrypted transfer of a secret 64-bit value used to ensure the integrity of the KSV list from the hardware to software. Additionally, a method for software to verify the integrity of status values that are passed unencrypted from hardware to the software is also provided. These distinct variations of the protocol are depicted in Figure 2-1 through Figure 2-4. In these figures, the software component is represented by endpoint C, and the graphics hardware by endpoint D. The endpoints of the protocol have key sets Ckeys and Dkeys, respectively.

In some integrated cases, the Graphics Hardware may use a set of Dkeys to authenticate more than one HDCP capable DVI port. In such cases, each port is accessed separately by means of an intra-Dksv index passed to the Upstream Protocol. This index is passed into the protocol via bits 4-6 of *Cmode* and is referred to as *index*.

Status Read

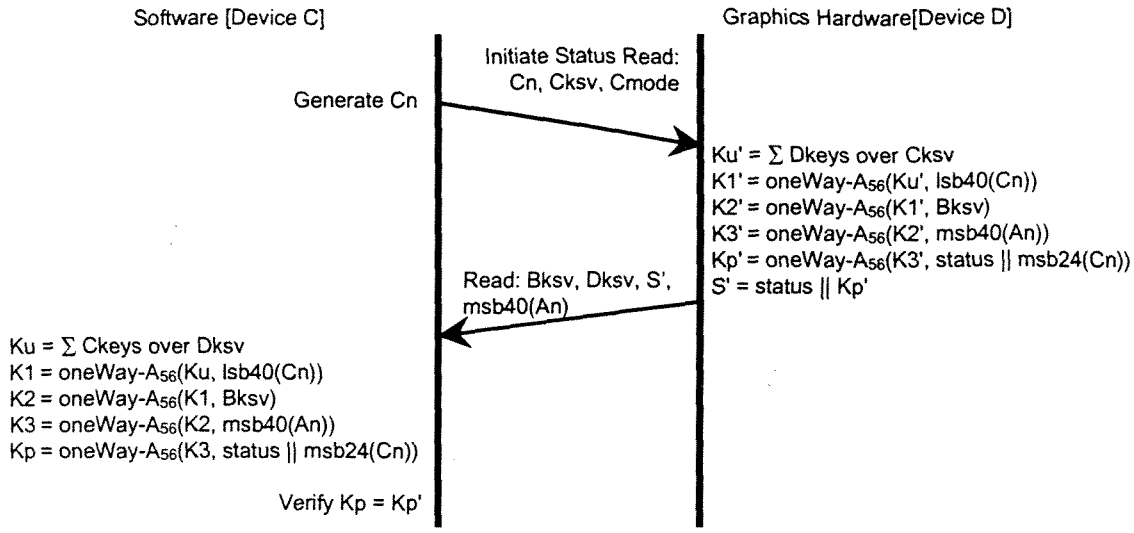

Figure 2-1. Upstream Protocol Status Read Without Connection State

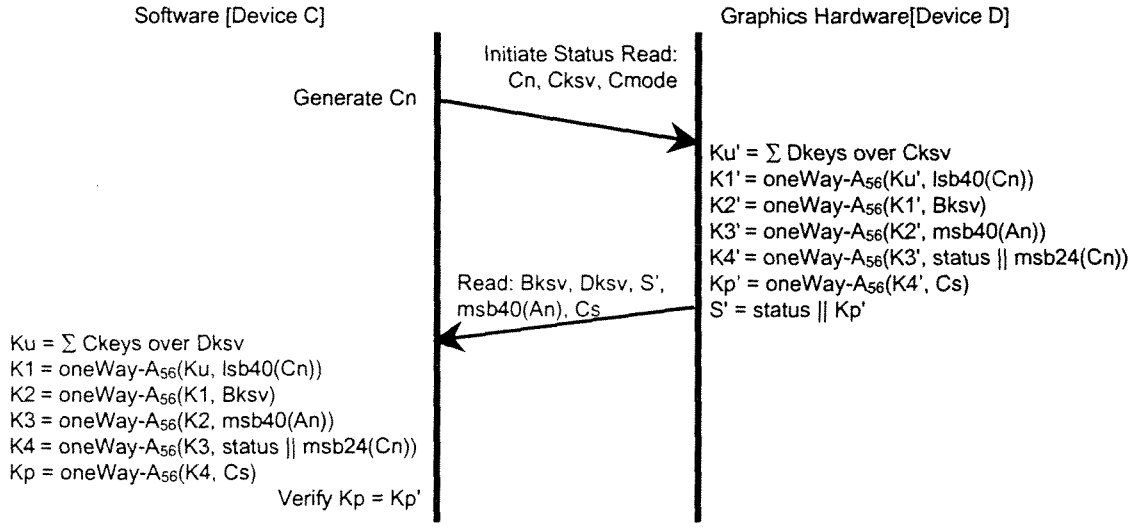

Figure 2-2. Upstream Protocol Status Read With Connection State

The status read protocol is shown in Figure 2-1 and Figure 2-2. Status bit 14 determines which of the two variations is performed. Software initiates the status read by transmitting to hardware its 40-bit key selection vector (*Cksv*), a 64-bit random value (*Cn*), and an indication that readStatus is the intended operation (*Cmode*). The hardware computes a sequence of 56-bit key values using the key summation and the one-way function oneWay-A. The values of *Cksv*, *Cn*, the key selection vector of the authenticated downstream receiver (*Bksv*), the 40 bits of the downstream *An*, 16 bits of status, and, if status bit 14 is set, 40 bits of connection state (*Cs*) contribute to the final computed value, *Kp'*, which is concatenated with the status bits. The concatenated value (*S'*) is returned to software along with msb40(An) the hardware key selection vector (*Dksv*), *Bksv* and , if status bit 14 is set, *Cs*. The software component first examines the returned status to determine if *Cs* is incorporated into the calculations, computes *Kp* from these values and compares the result to *Kp'*. The integrity of the received status word is verified when *Kp* equals *Kp'* and the returned *index'* (in *status*) equals *index* (in

Cmode). The composition of the 16-bit status, and *Cs* are defined in Table 5-1 and Table 5-2. The one-way function is defined in Section 3.

In the event that the HDCP capable DVI port is not transmitting or no such HDCP capable DVI port exists, the calculations proceed with arbitrary values in lieu of *Bksv* and msb40(*An*). These arbitrary values must be the same as those returned in the protocol to enable the software to verify *Kp* with *Kp'*.

All valid key selection vectors have a hamming weight of 20. The software must verify that the returned *Dksv* contains 20 1's and 20 0's. Otherwise, the returned *Kp'* shall be considered invalid.

Read M

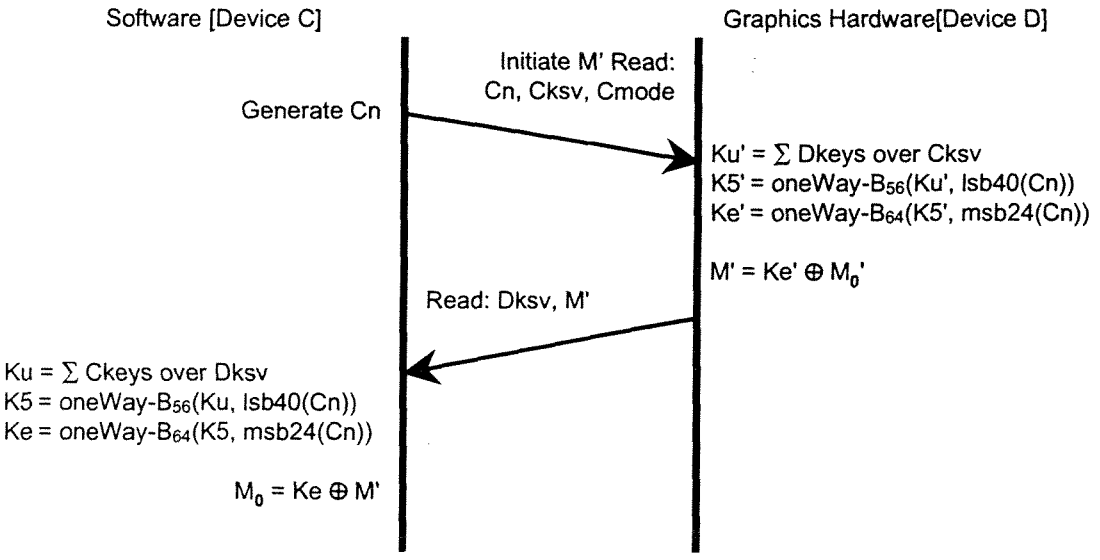

Figure 2-3. Upstream Protocol Read M

The HDCP specification enables revocation to be performed by source applications, and to do this it needs to verify the integrity of the key selection vector list that it receives from downstream video repeaters. The mechanism for this verification requires the computation of the verification value *V*. This value is a function of the secret value M_0, which is a confidential output of the HDCP cipher during downstream authentication. The second mode of the Upstream Protocol, readM, provides the means for the 64-bit M_0 value to be encrypted by the hardware for reading by the source application/revocation agent. Figure 2-3 illustrates this exchange.

It is possible that the readM operation may be engaged while the encryption enabled bit of the status is not set. In such cases, an arbitrary value may be substituted for M_0.

The readM operation is similar to the readStatus operation in that key selection vectors are exchanged and a series of values are computed using a one way function. In the readM case the one-way function oneWay-B is used. The final output of oneWay-B, *Ke'*, is a 64-bit value that is exclusive-ORed with the M_0 value. The result (M') is returned to software along with the transmitter's upstream key selection vector (Dksv). With these values, software is able to decrypt M' to obtain M_0, and in turn compute V' for the verification of the KSV list.

Read Z

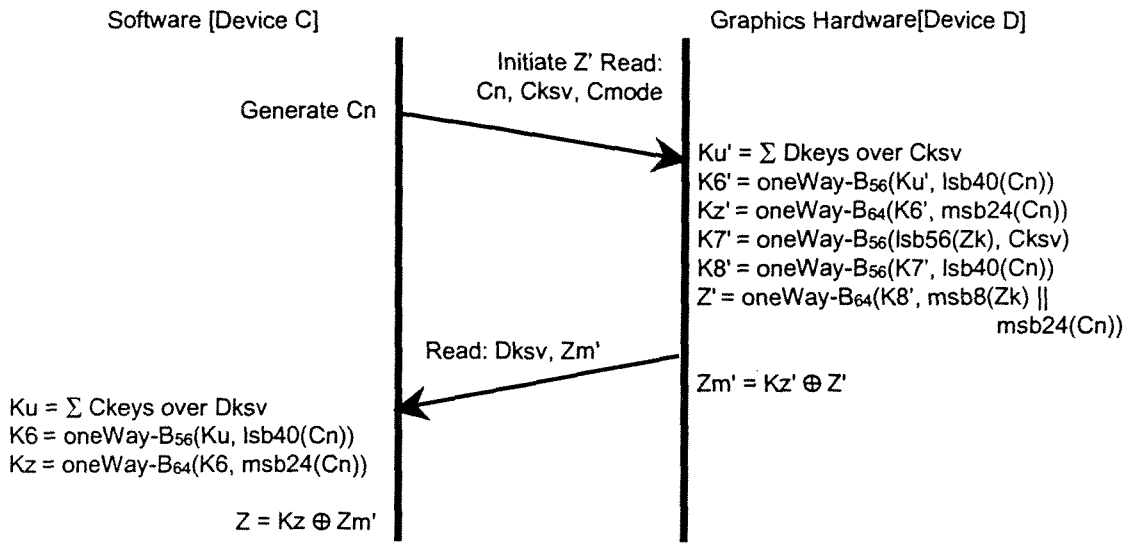

Figure 2-4. Upstream Protocol Read Z

The Upstream Protocol is designed to work in conjunction with solutions protecting the data path from the application to the video transmitter. In some solutions, the Upstream Protocol may provide initial keying material (*Z*). By providing *Z* to both the application and the data path decryption hardware, such systems can use the Upstream Protocol operations for much of the authentication work associated with establishing that encrypted content channel. Figure 2-4 illustrates this exchange.

The graphics hardware generates a 64-bit secret random or pseudo-random value, *Zk*. If the graphics hardware supports multiple content pipes, then there is a different *Zk* for each content pipe. The value of *Z* is calculated as a function of *Zk*, *Cn*, and *Cksv*.

The specifics of how *Z* is used as keying material depend on the specific method used to encrypted the content channel and, therefore, is beyond the scope of this specification. Software will use methods beyond the scope of this specification to determine if *Z* is used in such a content stream encryption mechanism, and how *Z* is applied if it is used. Furthermore, status bit 15 can be used to determine if the readZ operation is supported. For those implementations which do not use *Z*, an arbitrary value may be returned in lieu of Zm'.

3. One Way Functions

The one-way functions used in the Upstream Protocol are built from a set of four linear feedback shift registers (LFSRs) and a combining function as defined for the LFSR module of the HDCP cipher, with longer LFSRs. The two one-way functions differ only in the initialization of 100 bits of state (Table 3-2).

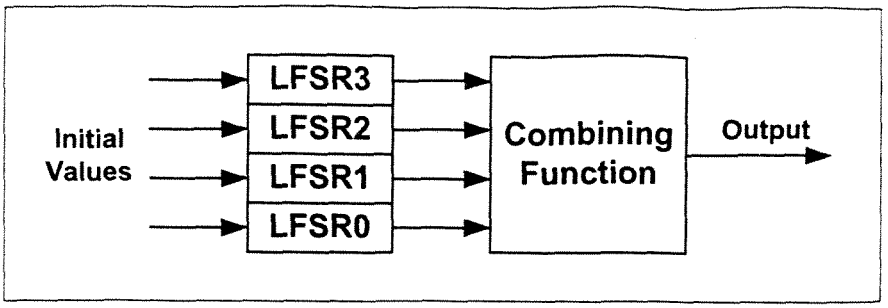

Figure 3-1. One Way Function

The upstream linear feedback shift register module consists of four LFSRs of different lengths and a combining function that produces a single bit stream from them. The combining function takes three taps from each LFSR. The generator polynomials and combining function taps for the LFSRs are specified in Table 3-1.

LFSR	Polynomial	Combining Function Taps		
		0	1	2
3	$x^{27}+x^{24}+x^{21}+x^{17}+x^{13}+x^{8}+1$	8	17	26
2	$x^{26}+x^{23}+x^{18}+x^{15}+x^{12}+x^{8}+1$	8	16	25
1	$x^{24}+x^{21}+x^{18}+x^{14}+x^{10}+x^{7}+1$	7	15	23
0	$x^{23}+x^{20}+x^{16}+x^{12}+x^{9}+x^{6}+1$	7	14	22

Table 3-1. LFSR Generation and Tapping

Figure 3-2 illustrates the tap locations of LFSR0 as well as the XOR term feedback into the least significant bit of LFSR0.

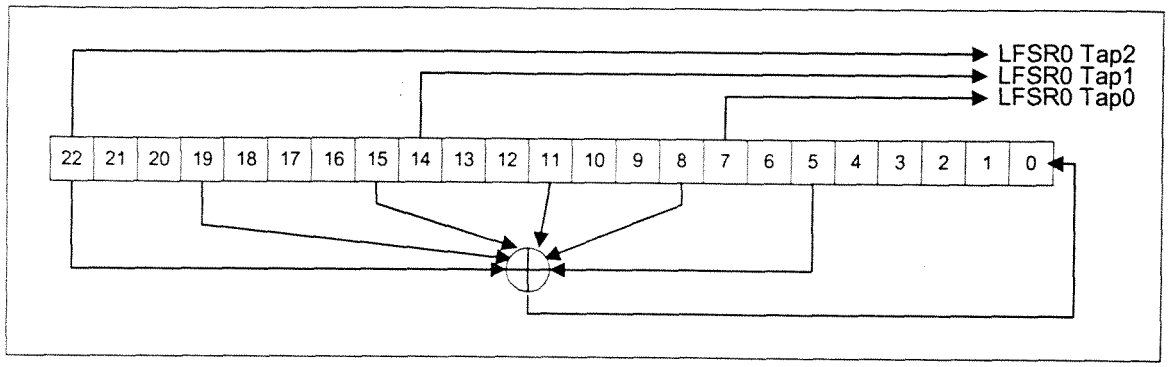

Figure 3-2. LFSR0

The combining function contains four cascaded shuffle networks, each of which includes two state bits. One tap from each of the four LFSRs is exclusive ORed together to form the data input to the first shuffle network. One tap from each of the four LFSRs is used as the select input to one of the four shuffle networks. The output of the fourth shuffle network is exclusive ORed together with one tap from each of the LFSRs. The Combiner Function illustrated in Figure 3-3.

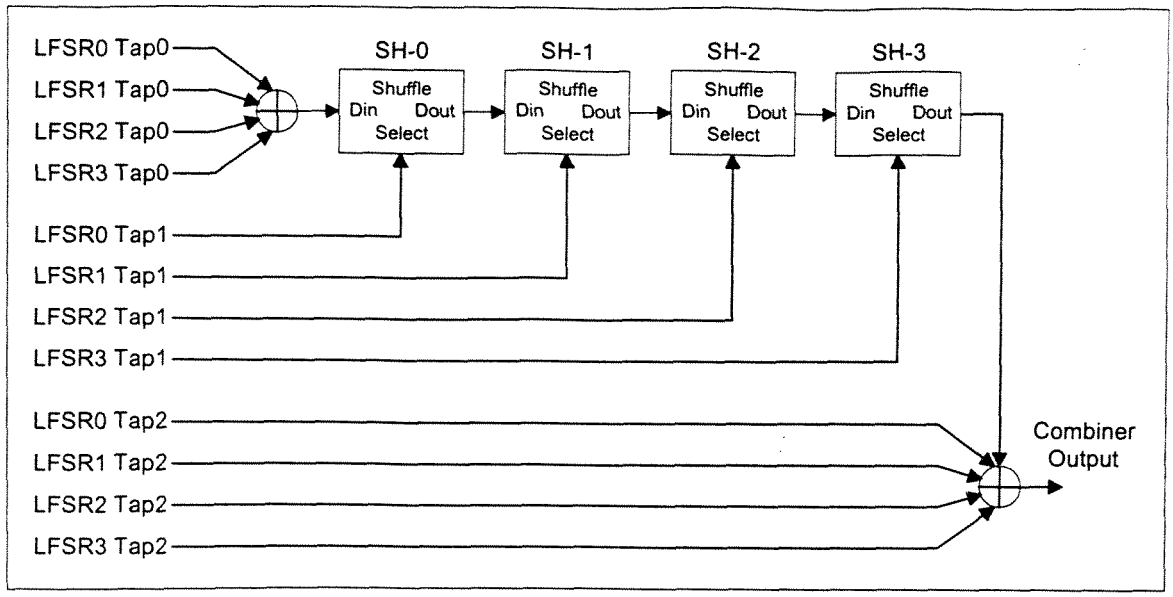

Figure 3-3. LFSR Module Combiner Function

The shuffle network is represented schematically in Figure 3-4. If the shuffle network contains the ordered pair of boolean values (A, B) and has boolean data input D and selection input S, the S value controls the next state. If S is zero, it outputs A and assumes state (B, D). If S is one, it outputs B and assumes state (D, A).

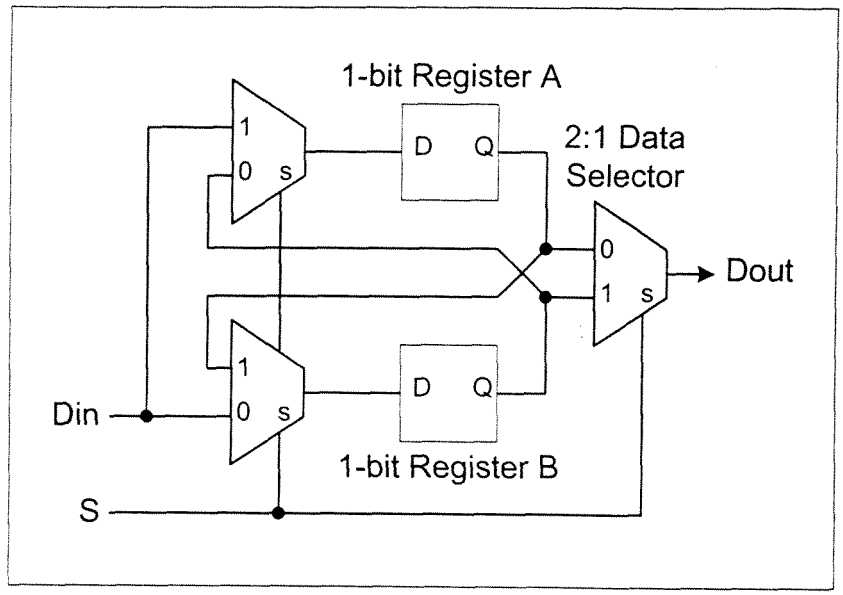

Figure 3-4. Shuffle Network

The LFSRs and combining function are initialized by a 56-bit key value and a 40-bit data value. The shuffle networks are each initialized with the same constant value. The initialization of the LFSRs is specified in Table 3-2. When the data value contains fewer than 40 bits, the 40-bit input value is zero-filled in the most significant bit locations.

	Bit Field	OneWay-A Initial Value	OneWay-B Initial Value
LFSR3	[26:22]	Data[39:35]	Data[34:30]
	[21]	*inverse of LFSR3 initialization bit* [9]	
	[20:14]	Data[34:28]	Data[29:23]
	[13:0]	Key[55:42]	Key[48:35]
LFSR2	[25:22]	Data[27:24]	Data[22:19]
	[21]	*inverse of LFSR2 initialization bit* [8]	
	[20:14]	Data[23:17]	Data[18:12]
	[13:0]	Key[41:28]	Key[34:21]
LFSR1	[23:19]	Data[16:12]	Data[11:7]
	[18]	*inverse of LFSR1 initialization bit* [5]	
	[17:14]	Data[11:8]	Data[6:3]
	[13:0]	Key[27:14]	Key[20:7]
LFSR0	[22:20]	Data[7:5]	Data[2:0]
	[19]	*inverse of LFSR0 initialization bit* [10]	
	[18:14]	Data[4:0]	Data[39:35]
	[13:7]	Key[13:7]	Key[6:0]
	[6:0]	Key[6:0]	Key[55:49]
Shuffle Networks	Register A	0	0
	Register B	1	1

Table 3-2. LFSR Module Initialization

Operation Sequence

The one-way functions are used to create 56-bit and 64-bit values. In every use, the LFSRs are loaded with the specified initial values and then clocked 32 times. After this 32 clock warm-up, the function is clocked 56 or 64 times, depending on the size of the outputted value. The value is taken serially from the combining function output least significant bit first.

4. Graphics Driver Requirements

The graphics driver facilitates both the upstream and the downstream protocols. The facilitation does not require any confidential values to be handled, nor does it require the driver to guarantee the integrity of any values. The combination of upstream and downstream protocols provides for the necessary confidentiality and integrity of values, without the imposition of a tamper resistant software component in the graphics driver.

HDCP Downstream Protocol

The graphics driver is responsible for the initiation and management of the downstream protocol. The protocol is started when the driver loads or when there is a hot plug event. Although the graphics driver facilitates the transfer of all protocol values, it does not handle revocation, and therefore does not completely implement the video transmitter state diagram of the HDCP specification. The downstream protocol values that are required for the source application to perform revocation are made

available through the Upstream Protocol. During the downstream facilitation, the driver maintains copies of those necessary values for later use. The graphics driver actions during all parts of the downstream authentication protocol are described in this section.

Driver load, link integrity check failure, and hot plug events		
Step	**Action**	**Comments**
1	Read *An*, *Aksv* from the transmitter	
2	Write *An*, *Aksv* to the receiver	
3	Read *Bksv* from the receiver	
4	Write *Bksv* to the transmitter	
5	Read and compare R_0 values from transmitter and receiver when available	
6	If attached to a video repeater, read the KSV list and *V* when available	

Driver two-second timer event (Link integrity check)		
Step	**Action**	**Comments**
1	Read and compare R_i values from transmitter and receiver	

Upstream Protocol

The graphics driver works in conjunction with the operating system to deliver an application programming interface to application software. The nature of this interface depends on the operating system.

5. Graphics Hardware Requirements

Table 5-1 defines a set of registers the graphics hardware must make available to software. In addition, implementations will have a method for initiating the downstream authentication protocol and also to enable the downstream encryption.

Name	Size in Bytes	Rd/Wr	Description
Aksv	5*	Rd	Transmitter KSV. The graphics driver reads this value, verifies that it contains 20 ones and 20 zeros, then writes the value to the video receiver.
An	8*	Rd	Link encryption session random number. This multi-byte value is copied to the video receiver by the graphics driver. Note: Reading the least significant byte of An forces a return to State A0 (Figure 2-4 of the HDCP specification[3]). The byte read is the least significant byte of the new An.
Bksv	5*	Rd/Wr	KSV of the video receiver that the video transmitter is encrypting data.
Btype	1*	Rd/Wr	This eight-bit value provides initial values for the data side of the HDCP Cipher. bits 7-1 reserved, must be zero.

[3] High-bandwidth Digital Content Protection, Version 1.0, Intel Corporation, February 17, 2000.

			bit 0: REPEATER capability bit reported by the attached device.
Cksv	5	Rd/Wr	Software KSV. Writing to this value triggers the upstream authentication sequence in the display device. Graphics hardware checks this value for 20 ones and 20 zeros.
Cmode	1	Rd/Wr	Upstream Protocol mode. This value must be written by software before the KSV is written. The most significant four bits specify an intra-Dksv index (index) to route the request. The least significant four bits specify the intended operation. Three operations are currently defined. All other values are reserved for future use. bit 7: reserved zero bits 6-4: zero-based intra-Dksv index to route the intended operation bits 3-0: mode: (1 = readStatus; 2 = readM; 3 = readZ; others reserved) Note: If bits 6-4 specify an invalid index, then this operation may be routed to any of the existing valid indices. Note: the following values returned in this register set are selected by bits 4-7 of Cmode: Actl, Aksv, An, Bksv, Btype, Cs, M, R_i, S, Zm'
Cn	8	Rd/Wr	Upstream exchange random number. This value must be written by software before the KSV is written.
Cs	5*	Rd	Connection State. See discussion below for further details. This value is required only if status bit 14 is 1. bits 39-29: implementation dependent connection state information bits 28-21: input plane flags bits 20-17: input pipe flags bit 16: at least one known Non-HDCP port is transmitting bits 15-8: reserved zeros bits 7-0: attach point flags
Dksv	5	Rd	Video transmitter upstream KSV. This value must always be available for reading. Valid KSVs contain 20 ones and 20 zeros, a characteristic that must be verified by application software before releasing protected content.
M'	8*	Rd	Encrypted M_0 value
Ri'	2*	Rd	Transmitter link integrity check value.
S'	9*	Rd	36:30 contain seven-byte Kp 38:37 status bits, always readable See discussion below for further details of the status bits.
Zm'	8*	Rd	Encrypted Z value. This value is required only if status bit 15 is 1.

* Indicates a separate instance for each HDCP-enabled DVI port indexed by Cmode.

Table 5-1. Required Hardware Registers

Cmode

Cmode specifies not only the upstream operation, but also selects which of possibly more than one HDCP-capable DVI port to route the request. This mechanism provides a means for the support of more than one HDCP-capable DVI port with a single set of Dkeys. Other mechanisms may be supported as well.

Connection State (Cs)

With graphics controllers increasing flexibility, there may be support for more than one display output from a given controller. As such, other outputs may be active on a controller and connected to displays or devices which may not be permitted for specific content being displayed.

The Connection State indicator enables a graphics controller to robustly relay its actual output configuration to applications enabling them to discover and evaluate the platform configuration and detect whether any unapproved display outputs are active. Furthermore, Connection State can indicate the presence of other permitted display such as those integrated with the device such as a laptop screen.

Connection State bits 0-7 are attach point flags. Each flag corresponds with a physical connection point to the graphics controller, or is always zero when not assigned. An attach point flag is set to one if a transmitter/codec is attached at the corresponding attachment point and may be sharing protected content stream(s) with this attachment point. These flags may be either global or restricted to a particular content stream path (i.e. describing which physical connection points may be receiving the same content stream(s)).

Connection State bit 16 is set if at least one known non-HDCP port is transmitting.

Connection State bits 17-20 are input pipe flags. Each flag corresponds to a physical input pipe that may be part of the content stream associated with this connection state. If less than four input pipes are supported, the remaining flags are always equal to zero.

Connection State bits 21-28 are input plane flags. Each flag corresponds to an input plane that may be part of the content stream associated with this connection state. If less than eight input planes are supported, the remaining flags are always equal to zero.

Connection State bits 29-39 provide optional additional state information associated with the mapping of content streams through the Graphics Controller to the physical connection points. This format of this additional information is implementation specific.

Status

Status is a 16-bit register that is returned by the readStatus operation as part of *S*. The signature, *Kp*, insures the integrity of the status bits returned. The definitions of the 16 bits of status are in Table 5-2.

Bit(s)	Description
15	1 if readZ is implemented.
14	1 if readStatus includes Connection State (Cs). The software must check this returned bit to determine whether Cs is part of the calculation of Kp.
13	1 if status bit 3 might not cover the entire scope of the content stream. If this bit is set, then Software must rely on Connection State or other means to assess the full scope of where the content streams flowing to this port are also flowing.
12	1 if this is an HDCP-compliant internal port and is currently transmitting.
11	reserved, zero
10-8	The maximum value of index. This is the maximum value of the intra-Dksv index passed in bits 6-4 of Cmode. If a higher value is passed in Cmode for this index, then the operation may be routed to any of the valid indices.
7	reserved, zero
6-4	The actual index this readStatus operation was routed to. This is equal to bits 6-4 of Cmode unless bits 6-4 of Cmode specified an invalid index.
3	1 if at least one unprotected port is transmitting. If bit 13 is also 1, then an unprotected port outside of the scope of this bit may be transmitting. In such a case, if bit 14 is 1, then the Software can perform the readStatus operation routed to all attachment points specified by the Connection State (i.e. corresponding to 1's in bits 0-7 of Cs), to assess the full scope of the content stream. Otherwise, if bit 14 is 0, then the Software must rely on other means to determine

	the full scope of the content stream.
2	1 if this is an HDCP-capable external port and is currently transmitting.
1	1 if a video repeater is attached to the HDCP-capable DVI port. This bit is 1 only if bit 2 is 1.
0	1 if encryption is enabled on the HDCP-capable external port or HDCP-compliant internal port.

Table 5-2. Definition of Status word

Table 5-3 provides examples of some valid combinations of the status bits.

Example Description	Bit 14	Bit 13	Bit 12	Bit 3	Bit 2	Bits 0-1
HDCP capable external port (e.g. DVI) is currently transmitting.	x	x	0	x	1	(*ext*)
HDCP capable external port (e.g. DVI) is currently not transmitting.	x	x	0	x	0	x
HDCP compliant (non user accessible) internal digital interconnect (e.g. LVDS) is currently transmitting.	x	x	1	x	0	(*int*)
Status bit 3 reports all unprotected ports within the scope of content stream within the graphics controller.	x	0	x	x	x	x
The information of status bit 3 must be supplemented by examining the connection state information and combining (OR) with status bit 3 of other ports corresponding to set bits in the port attach flags.	1	1	x	0	x	x
The information of status bit 3 cannot reliably determine if the content stream is emitting through an unprotected port.	0	1	x	0	x	x

0 = bit setting equals zero
1 = bit setting equals one
x = don't care or not applicable to this example
(*ext*) = bit settings reflect HDCP of external port, or zeros if no such settings are available
(*int*) = bit settings reflect HDCP of internal port, or zeros if no such settings are available

Table 5-3. Examples of Valid Status Bits

Figure 5-1 illustrates the hardware required to support the Upstream Protocol.

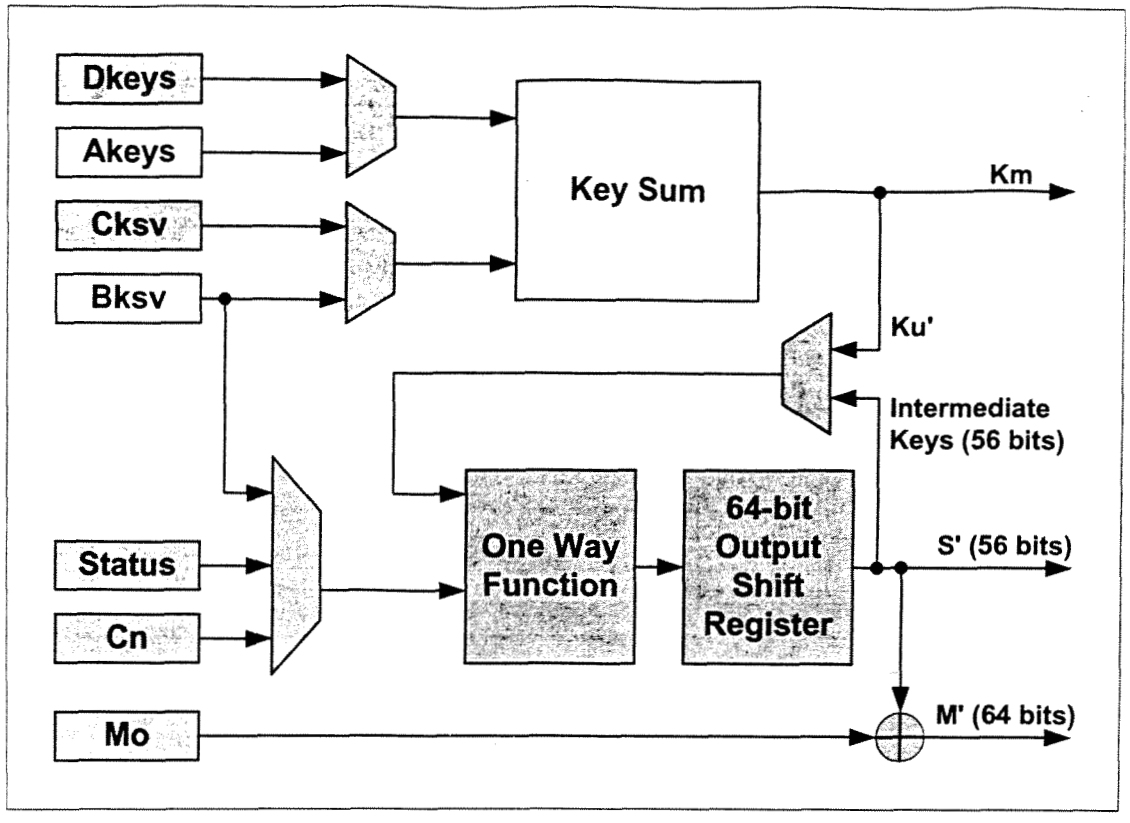

Figure 5-1. Graphics Hardware to Support the Upstream Protocol (shaded)

6. Source Application Requirements

A source application may be required by its content license to provide the link in the content protection chain to the HDCP output. This requires a set of keys to participate in the Upstream Protocol. Multiple applications may exist in the system, each with the capability to query the graphics system for the HDCP Upstream Protocol API. The graphics driver must implement the proper atomicity or exclusive access for this shared environment.

Figure 6-1 represents the state diagram that a source application implements when using the Upstream Protocol.

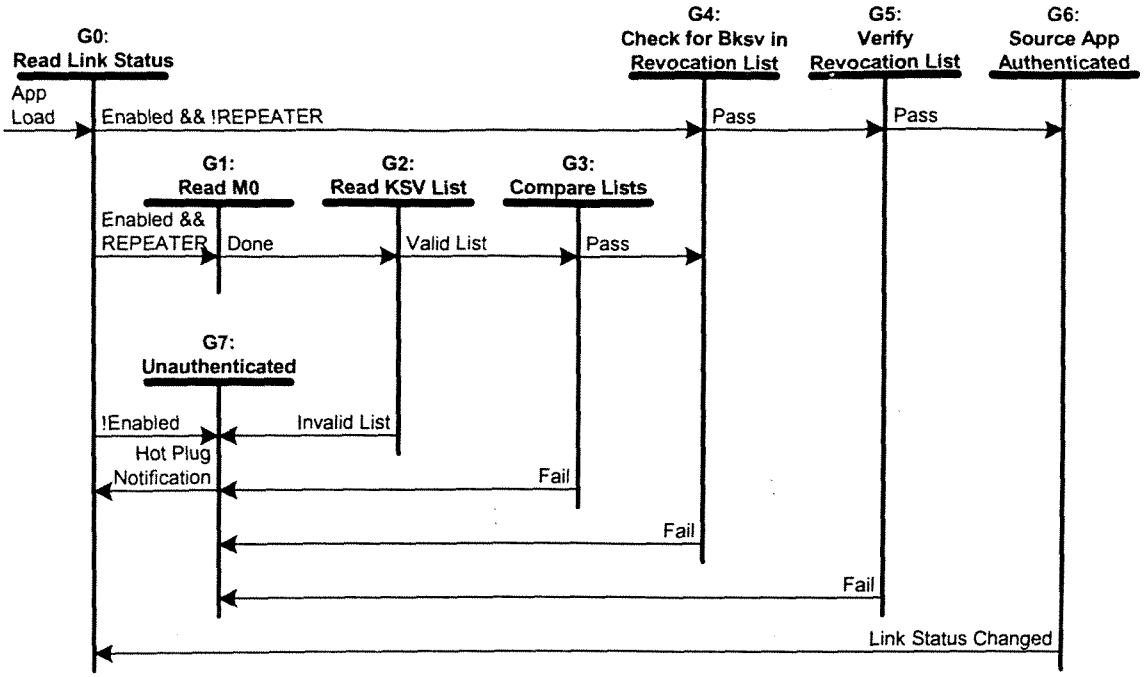

Figure 6-1. Source Application State Diagram

Transition Any State:G0. The source application initializes to State G0 when it loads.

State G0: Read Link Status. In this state the application queries the graphics driver for the HDCP interface, and makes the readStatus API call. The status returned dictates the transition out of this state.

Transition G0:G1. This transition is made if the DVI link has encryption enabled and the attached display device is a video repeater.

Transition G0:G4. This transition is made if the DVI link has encryption enabled and the attached display is not a video repeater.

Transition G0:G7. This transition is made when the driver does not support the HDCP API or if the driver reports that encryption is not enabled on the DVI link for any reason.

State G1: Read M_0. In this state, the source application makes the readM0 API call. The return value M' must be decrypted.

Transition G1:G2. The source application transitions to State G2 after decrypting M_0.

State G2: Read KSV List. In this state the application makes the readKSVList API call. With M_0 the application computes the list verification value V and compares this value to the value V' returned with the KSV list by the graphics driver.

Transition G2:G3. This transition is made when the KSV list returned by the graphics driver is valid as indicated by $V == V'$.

Transition G2:G7. This transition is made when the KSV list returned by the graphics driver is not valid as indicated by the miscompare of V and V'. The application may protect against I^2C errors with a retry through an HDCP API, forcing the graphics driver to re-read the list from the video receiver.

State G3: Compare Lists. In this state the application compares the current revocation list with the validated KSV list.

Transition G3:G4. This transition is made if no members of the KSV list are present in the current revocation list.

Transition G3:G7. This transition is made if any members of the KSV list are present in the current revocation list.

State G4: Check for Bksv in Revocation List. In this state the application verifies that the *Bksv* of the attached video receiver (or video repeater) is not present in the current revocation list.

Transition G4:G5. This transition is made if *Bksv* is not present in the current revocation list.

Transition G4:G7. This transition is made if *Bksv* is present in the current revocation list.

State G5: Verify Revocation List. In this state the application verifies the signature of the current revocation list, as described in the HDCP specification.

Transition G5:G6. This transition is made if the current revocation list is valid.

Transition G5:G7. This transition is made if the current revocation list is not valid.

State G6: Source App Authenticated. In this state the source application has authenticated the collection of attached video receivers and may deliver protected content through the video subsystem. The source application may periodically verify that the link remains encrypted by reading status through an HDCP API.

Transition G6:G0. This transition is made whenever the application determines that the link may no longer encrypted under the original downstream authentication. The application directly observes changes to the link encryption status (e.g. *An*, *Cs*, status bits, M_0) through an HDCP API. The application may also be notified of hot plug, power state change, and link failures (Ri != Ri') by the graphics driver.

State G7: Unauthenticated. In this state the application has determined that protected content should not be delivered through the graphics subsystem.

Transition G7:G0. This transition is made when the graphics driver signals that a hot plug, power state change, or link failure event has occurred.

7. Key Storage

HDCP keys must be protected by either cryptographic or physical means. Furthermore, *Akeys* and *Dkeys* must be bound together in a manner which prevents their substitution. The binding can be either physical or cryptographic in nature.

8. Confidentiality and Integrity of Values

Table 8-1 identifies the requirements of confidentiality and integrity for values within the protocol. A *confidential* value must never be revealed. The *integrity* of many values in the system is protected by fail-safe mechanisms of the protocol. Values that are not protected in this manner require active measures beyond the protocol to ensure integrity. Such values are noted in Table 8-1 as requiring integrity.

Value	Size (Bytes)	Confidentiality Required[4]?	Integrity Required[4]?	Function
Cksv	5	No	No	Source application's Key Selection Vector
Cn	8	No	No	Pseudo-random value sent to video transmitter by source application
Cmode	1	No	No	Exchange type requested by source application of video transmitter
Cs	5	No	Yes	Connection State
Dksv	5	No	Yes	Video transmitter's upstream KSV
Ku, Ku'	7	Yes	Yes	Upstream matrix key
Ckeys	280	Yes	Yes	Source application's endpoint keys
Dkeys	280	Yes	Yes	Video transmitter's upstream endpoint keys
Status	2	No	Yes	Encryption enable and REPEATER status from the video transmitter
K1, K2, K3, K4, K5, K6, K7, K8	7	Yes	Yes	Source application's intermediate key values
K1', K2', K3', K4', K5', K6', K7', K8'	7	Yes	Yes	Video transmitter's intermediate key values
Kp	7	Yes	Yes	Source application's status verification value
Kp'	7	No	No	Video transmitter's status verification value
Ke	8	Yes	Yes	Source application's encryption key for M_0
Ke'	8	Yes	Yes	Video transmitter's upstream encryption key for M_0
Ku	8	Yes	Yes	Source application's matrix key result
Ku'	8	Yes	Yes	Video transmitter's matrix key result
Kz	8	Yes	Yes	Source application's encryption key for Z
Kz'	8	Yes	Yes	Video transmitter's upstream encryption key for Z
M_0	8	Yes	Yes	M_0 value from video transmitter
M'	8	No	No	Encrypted M_0 value from video transmitter
P	5	No	Yes	Content stream pipe identifier (non- integrated case only).
Z	8	Yes	Yes	Source application's optional supplemental key material
Z'	8	Yes	Yes	Video transmitter's optional supplemental key material
Zk	8	Yes	Yes	Video transmitter's random or pseudo random seed for Z'.
Zm'	8	No	No	Encrypted Z' from the video transmitter

Table 8-1. Confidentiality of Values

[4] According to the robustness rules in the HDCP Adopter's License.

Appendix A. Test Vectors

Table A-1 provides facsimile key information for test purposes. Two keys sets for software (C1 and C2) are provided and two keys sets for graphics hardware (D1 and D2) are provided, along with a one's complement checksum of each of the 40 key sets for accuracy check.

	Key Set C1	Key Set C2	Key Set D1	Key Set D2
KSV	b86646fc8c	f42546e22f	fc5d32906c	c6cb5058f6
Key 0	bf9323eba7bd83	cdc9d9ce27e6e0	a93468cae14ebd	f325e845ec0475
Key 1	9f4618fb1fddcd	7efad4b557d488	e3d48c7f66c84c	c8ea60a2c614a0
Key 2	af9af9f70a4016	4cbbdcb33fb4a8	b04b1a41fd278c	e71952c803acac
Key 3	a6486e54e184e5	fd0e1a13c7f916	43401fd2faa3e8	44883a2430039e
Key 4	9ae6c3b7ab7997	4180c45dc71248	dee22935c4ba78	b952c63eef2602
Key 5	3fac11e60feab9	8bff8b99dfe266	fc17073786de76	3248a5402f2c5d
Key 6	0fc296be6169fd	15d8de49f9c23e	19ed1fa04398a3	d1cb314d852d1b
Key 7	a60a6b7046bdc7	b8571b74045e5e	4831895e08a757	1c0930e3c990f8
Key 8	d97ab64ded4213	284a6d3b09e1d5	e44fde1a332a07	d08f4d09ba0e99
Key 9	9a98ca3cb335d8	6e207738e6a772	b69ce091ff6b0b	618c9bf1b7d40c
Key 10	aec8d340924cd2	1dbe6418a5f39d	41a098bf74eb63	d94809a5b9fa51
Key 11	24063db7783b67	2e598a7ad02be4	762a1a2e7b5d88	5d9d07cd0c9ee7
Key 12	74ec773c2e5306	259ca2d605d330	9da0d25b40d3f8	497a0a73085037
Key 13	e67ab5293cdb6b	486b5feadad839	f2fa190db288eb	240fc5121bf75c
Key 14	44634e169974ee	c11420a6cc4290	c9e7a970b1d9bc	fa3e5d64306a91
Key 15	675d2f23a50021	7623fe830a5c9c	ed8e4a7734f66a	e5998a6a8fe53f
Key 16	840e353bbe276b	a2ce3c7ad77689	5e4831ab0cf398	d708396c888cbf
Key 17	faf3ea7f7e6fe5	d042110c098bdc	8cdc4665b81aab	d517260f41882a
Key 18	a66c5ef761f745	f972af7e10f74d	d689ebf39b0dd9	a2ee7277d142a3
Key 19	3281b7d3fed3a6	7108fc56a2ee42	58258915a41885	61596e405e7eed
Key 20	0c18cf5d267ad9	b857ea6eefa4d0	4d19c0ed0e3a84	0f8a593b3add20
Key 21	3c4bfb02724239	133c20197b4106	b99bb514d3c0f9	09ae90e92456f6
Key 22	1e59b589ed36a5	5da94a02426f8e	6192f0cd3eefac	f75f00d4d567b5
Key 23	efd5979c3c8967	74fdc6a24c6d62	d426ea14cabd38	26c272e6a701bf
Key 24	8c8cb0b2c56787	efbfa2cfab3739	c258b2bba653ca	c0c0871320305c
Key 25	3271dbf201eee8	d976507abc3a13	546053178d15c4	74d3a22169fe9d
Key 26	638ad2b0a05aea	ea21a8310e052f	bb2a9f5f373af3	8a81710173b103
Key 27	ba9d886613d86b	7cd4c5be0a234d	f2e9dfa1681b27	e43bb9c1665277
Key 28	aad73506a50c09	c2f02a39b4b616	bdddf7b276351d	f911c8dd5e8a45
Key 29	30b80cc15a98bb	5330aa0668bcbf	bf543efa74e4e2	383bdd378c2b35
Key 30	6059cf02f46ca1	88b1758b580bd3	9d3b1489fb5f28	6b3d07b6e85577
Key 31	091bfd1f2c67c0	4ec1293fcce288	4a2570fec02ccf	6be30b334b7948
Key 32	6ee12b81562882	2aba10f24399b8	e582d46f477ecb	a828cb19016ee1
Key 33	7ebeea3a8c94ee	83493ceb0a9415	42f0661748bbcd	a5f0e70c54947d
Key 34	4a7edad3ce070a	abfd1cc9aafb2d	2f9a4481c827ef	11e2fb69128645
Key 35	90fca1ed41f1dd	fb55bec3b74a6f	99bbc41951c1cf	ec99d64df8a440
Key 36	2bcb7d6b167472	39c143043cdb6f	b4c678a16939e9	4e43819924bdf7
Key 37	91581d525f5130	2174e9d7f8158a	0b7a651c23eb0d	e8e55f6b7370d3
Key 38	cf6531384fe395	d8e773fda37975	0e20667be29368	f4a293e35b3fcc
Key 39	bf745d37be3dae	182dd7d8893c4f	dbaac1467e10ac	204bd804d27791
CHECKSUM	78efb77dde0f94	f52a6edcad31b8	73ed215ed5f682	a4b2d11aef2be0

Table A-1. Facsimile Device Keys

Table A-2 illustrates the calculation of *Ku/Ku'* with facsimile device key sets C1 and D1. A selection of 20 of the device's private keys are combined using 56-bit binary addition. The selection of private

keys combined corresponds to the bit indices of the 1's within the other device's key selection vector. For example, facsimile D1 key selection vector is fc5d32906c of which the following 20 bits are set: 2, 3, 5, 6, 12, 15, 17, 20, 21, 24, 26, 27, 28, 30, 34, 35, 36, 37, 38, and 39. Therefore, facsimile C1 adds together its following private keys to calculate Ku: 2, 3, 5, 6, 12, 15, 17, 20, 21, 24, 26, 27, 28, 30, 34, 35, 36, 37, 38, and 39.

Facsimile Device C1 Sum of Keys Calculation		**Fascimile Device D1 Sum of Keys Calculation**	
Key 2	af9af9f70a4016	Key 2	b04b1a41fd278c
Key 3	a6486e54e184e5	Key 3	43401fd2faa3e8
Key 5	3fac11e60feab9	Key 7	4831895e08a757
Key 6	0fc296be6169fd	Key 10	41a098bf74eb63
Key 12	74ec773c2e5306	Key 11	762a1a2e7b5d88
Key 15	675d2f23a50021	Key 12	9da0d25b40d3f8
Key 17	faf3ea7f7e6fe5	Key 13	f2fa190db288eb
Key 20	0c18cf5d267ad9	Key 14	c9e7a970b1d9bc
Key 21	3c4bfb02724239	Key 15	ed8e4a7734f66a
Key 24	8c8cb0b2c56787	Key 17	8cdc4665b81aab
Key 26	638ad2b0a05aea	Key 18	d689ebf39b0dd9
Key 27	ba9d886613d86b	Key 22	6192f0cd3eefac
Key 28	aad73506a50c09	Key 25	546053178d15c4
Key 30	6059cf02f46ca1	Key 26	bb2a9f5f373af3
Key 34	4a7edad3ce070a	Key 29	bf543efa74e4e2
Key 35	90fca1ed41f1dd	Key 30	9d3b1489fb5f28
Key 36	2bcb7d6b167472	Key 35	99bbc41951c1cf
Key 37	91581d525f5130	Key 36	b4c678a16939e9
Key 38	cf6531384fe395	Key 37	0b7a651c23eb0d
Key 39	bf745d37be3dae	Key 39	dbaac1467e10ac
RESULT (*Ku*):	a25321f0ee8d21	**RESULT (*Ku'*):**	a25321f0ee8d21

Table A-2. Sample *Ku* and *Ku'* Calculation

Table A-3 illustrates sample calculations of the readStatus operation without Connection State using various combinations of device key sets C1, C2, D1, and D2.

	C1 – D1	**C2 – D2**	**C2 – D1**	**C2 – D2**
status	0105	0115	0008	0007
Cn	2c72677f652c2f27	f0fa8bc54b981cca	bd4bac10c902d2bd	f24977262e7ed2fe
Bksv	e72697f401	511ef21acd	511ef21acd	e72697f401
An	34271c130c	445e62a53a	83bec2bb01	0351f71754
Ku	a25321f0ee8d21	2232a75b461f46	b92f225bfa01d7	d04b7ae589bc76
K1	eb09adb5f6dc25	c424fbf6db045c	623e7c0e7fb070	6619ae14c42333
K2	71ebb3cc7693d4	423ba5fd5fecf0	ecebd28a716c30	130412205bb0b6
K3	fd27048ba34cc4	790514885ea2dd	f9af695ad7dae9	33f4b64a511034
Kp	03e6205ba71568	b253c3c4da01a5	2142a625581f42	92181a1a05bea3

Table A-3. ReadStatus Without Connection State

Table A-4 illustrates sample calculations of the readStatus operation with Connection State using various combinations of device key sets C1, C2, D1, and D2.

	C1 – D1	C2 – D2	C2 – D1	C2 – D2
status	1105	1115	1008	1007
Cn	2c72677f652c2f27	f0fa8bc54b981cca	bd4bac10c902d2bd	f24977262e7ed2fe
Bksv	e72697f401	511ef21acd	511ef21acd	e72697f401
An	34271c130c	445e62a53a	83bec2bb01	0351f71754
Cs	0000000001	0000000003	2badd40005	b5073c0003
Ku	a25321f0ee8d21	2232a75b461f46	b92f225bfa01d7	d04b7ae589bc76
K1	eb09adb5f6dc25	c424fbf6db045c	623e7c0e7fb070	6619ae14c42333
K2	71ebb3cc7693d4	423ba5fd5fecf0	ecebd28a716c30	130412205bb0b6
K3	fd27048ba34cc4	790514885ea2dd	f9af695ad7dae9	33f4b64a511034
K4	2e02408cb8cf44	c2d7bf6d5fd134	36e7a6b5f05915	e80edbb5a771ce
Kp	b1c0a2a4d66570	90ff5055d38a4b	b689fb2bb760dd	689f3c2e278b99

Table A-4. ReadStatus With Connection State

Table A-5 illustrates sample calculations of the readM operation using various combinations of device key sets C1, C2, D1, and D2.

	C1 – D1	C1 – D2	C2 – D1	C2 – D2
M0	504fdf2425befed4	57631a035123cc07	9946ac996e28999f	fa93939bc65d8a2d
Cn	36d36579ba89542d	65a668e67a75b445	06327afcf5768049	a3adeba3472d29e6
Ku	a25321f0ee8d21	2232a75b461f46	b92f225bfa01d7	d04b7ae589bc76
K5	5bc1db127f1e27	caa57c231daace	ce45d423d9e5ac	e2469ee0fc805b
Ke	da4245977574bf86	bde1ef1d0d5439d1	2792ac82bef45d7f	2e47be37b9f7c23c
M	8a0d9ab350ca4152	ea82f51e5c77f5d6	bed4001bd0dcc4e0	d4d42dac7faa4811

Table A-5. ReadM

Table A-6 illustrates sample calculations of the readZ operation using various combinations of device key sets C1, C2, D1, and D2.

	C1 – D1	C1 – D2	C2 – D1	C2 – D2
Zk	5eba3c4a60abe7da	1435e6dc67bbd3a4	d0d7ce7de9f8ef68	4523afe2506a8407
Cn	06327afcf5768049	36d36579ba89542d	a3adeba3472d29e6	65a668e67a75b445
Ku	a25321f0ee8d21	2232a75b461f46	b92f225bfa01d7	d04b7ae589bc76
K6	d307089a5e014c	417f4af0c26f6e	b47d1e9c734966	a3a05e5bac7e57
Kz	4cf99e93e03bfbc2	a0ae755a534c2de4	99509326a8a2f355	6ee3dbaade15d550
K7	30bbb798f87e50	237066e1c6f58d	3dfaadf2c5a08c	4680a23de4d953
K8	068b482481de44	51441472e73336	9bdb14b839d8f0	0a131c77eb3faa
Z	2efae880e1575606	cd79ff8b2a6f2fbf	8ed5ec1371b8128f	6e10bf73ac238654
Zm	62037613016cadc4	6dd78ad17923025b	17857f35d91ae1da	00f364d972365304

Table A-6. ReadZ

Table A-7 through Table A-22 illustrate in more detail the calculations for the cases of using device key sets C1 and D1.

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	11cd21	13c3ba	165b21f	3fda894	1	0	1	1	1	0	01	01	01	01	
1	239a42	278775	2cb643f	7fb5128	1	0	0	1	1	1	10	10	10	11	
2	473484	4f0eeb	196c87e	7f6a251	0	0	0	0	0	1	01	11	01	01	
3	0e6909	9e1dd7	32d90fd	7ed44a3	1	1	1	0	1	0	10	10	11	00	
4	1cd213	3c3bae	25b21fa	7da8946	1	0	1	0	1	1	11	00	11	01	
5	39a426	78775d	0b643f4	7b5128d	1	1	0	0	0	0	11	01	01	10	
6	73484d	f0eeba	16c87e9	76a251a	1	1	1	1	0	1	11	11	10	00	
7	66909a	e1dd74	2d90fd2	6d44a35	0	0	0	1	1	0	11	11	01	10	
8	4d2134	c3bae8	1b21fa4	5a8946b	0	1	0	1	0	0	10	11	10	01	
9	1a4268	8775d1	3643f49	35128d7	0	0	1	0	0	0	00	11	01	11	
10	3484d0	0eeba2	2c87e93	6a251af	1	0	0	1	0	1	00	10	11	10	
11	6909a1	1dd745	190fd27	544a35e	1	0	0	1	0	0	01	01	10	11	
12	521343	3bae8b	321fa4e	28946bd	1	0	0	1	1	0	11	00	01	11	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	2187ec	4581c9	12775c0	35edca8	1	0	0	1	1	1	01	00	01	10	
28	430fd9	8b0393	24eeb81	6bdb951	0	0	0	0	0	0	11	00	00	11	
29	061fb3	160727	09dd702	57b72a3	0	1	0	0	1	1	10	01	00	10	
30	0c3f67	2c0e4f	13bae05	2f6e547	1	0	0	0	1	1	00	11	00	01	
31	187ece	581c9e	2775c0a	5edca8e	0	0	1	0	1	0	01	10	10	00	0
32	30fd9c	b0393d	0eeb815	3db951c	0	1	1	0	0	1	00	01	11	00	1
33	61fb39	60727b	1dd702b	7b72a38	0	0	1	0	1	1	00	10	10	10	0
34	43f673	c0e4f7	3bae056	76e5470	1	0	1	1	0	1	00	00	11	01	1
35	07ece7	81c9ef	375c0ad	6dca8e0	0	1	1	1	1	0	10	00	10	10	0
36	0fd9cf	0393de	2eb815a	5b951c0	0	0	1	1	1	0	01	00	01	00	0
37	1fb39e	0727bd	1d702b5	372a380	1	0	0	0	1	1	00	10	00	01	1
38	3f673d	0e4f7b	3ae056b	6e54700	0	0	1	0	0	0	01	00	10	00	0
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	3f84e5	b7a87a	371278b	59eab1d	1	1	0	1	1	1	01	01	10	11	0
78	7f09cb	6f50f5	2e24f17	33d563b	1	0	0	0	0	0	11	00	11	01	0
79	7e1396	dea1ea	1c49e2f	67aac77	0	1	0	1	0	1	11	01	10	11	0
80	7c272d	bd43d5	3893c5e	4f558ee	1	0	0	0	1	0	10	10	01	11	1
81	784e5a	7a87aa	31278bc	1eab1dc	0	0	1	1	0	1	01	01	10	11	1
82	709cb5	f50f55	224f179	3d563b9	1	1	0	0	0	0	00	10	01	11	0
83	61396a	ea1eaa	049e2f2	7aac772	0	1	0	0	1	1	01	00	11	10	1
84	4272d4	d43d55	093c5e5	7558ee4	0	1	1	0	1	0	10	00	01	11	0
85	04e5a9	a87aaa	1278bcb	6ab1dc8	0	0	1	0	1	1	01	00	00	11	1
86	09cb53	50f555	24f1797	5563b91	0	0	1	1	1	1	00	01	00	01	1
87	1396a6	a1eaab	09e2f2e	2ac7722	0	1	0	1	0	0	00	00	10	00	1
88	272d4c	43d557	13c5e5c	558ee44	0	1	0	1	0	0	00	00	00	01	
K1	**eb09adb5f6dc25**														

Table A-7. Detailed ReadStatus C1-D1 Without Connection State K1

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	005c25	fd17db	1b2dadb	71cbac2	1	0	1	0	0	0	01	01	01	01	
1	00b84a	fa2fb6	365b5b6	6397584	1	1	0	0	1	0	10	11	10	10	
2	017094	f45f6d	2cb6b6d	472eb09	1	1	1	0	1	1	01	11	11	00	
3	02e128	e8beda	196d6db	0e5d612	1	1	1	1	0	0	10	11	11	10	
4	05c251	d17db4	32dadb7	1cbac25	0	0	1	0	1	1	11	01	11	01	
5	0b84a3	a2fb69	25b5b6f	397584a	0	0	0	1	1	1	01	11	01	10	
6	170947	45f6d3	0b6b6df	72eb094	1	1	0	1	0	1	10	01	10	11	
7	2e128e	8beda7	16d6dbe	65d6129	0	0	0	1	1	0	01	10	01	11	
8	5c251d	17db4f	2dadb7c	4bac253	1	1	0	1	0	1	10	01	00	11	
9	384a3b	2fb69e	1b5b6f9	17584a7	1	0	1	1	1	0	01	10	01	01	
10	709477	5f6d3d	36b6df3	2eb094f	0	0	0	0	1	1	10	11	00	11	
11	6128ef	beda7b	2d6dbe6	5d6129e	0	0	0	1	0	1	00	11	10	01	
12	4251df	7db4f7	1adb7cc	3ac253d	0	1	1	1	1	0	00	01	01	10	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	6fbfeb	7bfe7b	3e64111	29edf22	1	0	0	1	0	1	01	11	00	00	
28	5f7fd6	f7fcf7	3cc8222	53dbe45	0	0	1	1	0	0	11	01	01	00	
29	3effac	eff9ef	3990444	27b7c8a	0	0	1	1	1	1	01	10	11	00	
30	7dff59	dff3de	3320889	4f6f914	0	0	1	1	0	1	00	11	01	10	
31	7bfeb3	bfe7bc	2641112	1edf228	1	1	1	1	0	0	00	01	11	01	1
32	77fd67	7fcf79	0c82224	3dbe451	0	1	1	1	0	1	10	00	11	11	0
33	6ffacf	ff9ef2	1904449	7b7c8a3	0	1	1	1	0	1	01	00	10	11	0
34	5ff59e	ff3de5	3208893	76f9147	1	0	1	0	0	1	00	10	00	11	1
35	3feb3c	fe7bcb	2411127	6df228f	0	1	1	0	1	1	10	00	01	01	0
36	7fd679	fcf796	082224e	5be451f	0	1	1	1	0	1	01	00	00	10	1
37	7facf2	f9ef2c	104449d	37c8a3f	1	0	0	1	0	0	00	10	00	01	0
38	7f59e5	f3de58	208893a	6f9147f	0	0	1	1	0	0	01	01	00	10	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	2842c9	33550f	053e990	7fcbce1	0	1	1	0	1	0	01	11	10	01	1
78	508593	66aa1e	0a7d321	7f979c3	1	0	0	1	1	0	00	11	11	10	1
79	210b27	cd543d	14fa642	7f2f386	1	0	0	0	1	1	01	01	11	01	1
80	42164f	9aa87b	29f4c84	7e5e70d	1	0	0	1	1	0	11	10	01	10	1
81	042c9f	3550f7	13e9909	7cbce1b	1	1	0	0	0	1	11	11	00	01	0
82	08593f	6aa1ee	27d3212	7979c37	1	0	1	1	1	1	11	11	01	00	0
83	10b27e	d543dd	0fa6424	72f386f	1	0	0	0	0	1	11	11	10	10	0
84	2164fc	aa87ba	1f4c849	65e70df	0	0	1	1	0	1	11	11	01	11	1
85	42c9f9	550f75	3e99093	4bce1be	0	1	1	0	1	0	01	11	11	01	1
86	0593f3	aa1eeb	3d32127	179c37c	0	0	0	0	1	0	00	11	11	11	1
87	0b27e7	543dd6	3a6424f	2f386f8	0	1	0	0	0	1	00	10	11	11	0
88	164fcf	a87bad	34c849f	5e70df0	1	1	1	0	0	1	00	00	11	11	
K2	**71ebb3cc7693d4**														

Table A-8. Detailed ReadStatus C1-D1 Without Connection State K2

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	0b13d4	0cf1da	1c3bb3c	1b09c7a	1	0	0	1	1	0	01	01	01	01	
Load															
1	1627a8	19e3b4	3877679	36138f5	0	1	0	1	1	0	11	00	10	11	
2	2c4f50	33c769	30eecf3	6c271eb	1	0	1	1	0	1	10	10	01	10	
3	589ea1	678ed2	21dd9e7	584e3d6	0	1	0	1	1	0	11	01	10	01	
4	313d43	cf1da5	03bb3ce	309c7ad	1	1	0	0	1	0	10	10	11	10	
5	627a86	9e3b4a	077679c	6138f5a	1	1	1	0	1	1	01	01	11	01	
6	44f50c	3c7694	0eecf38	4271eb5	0	0	1	0	0	1	10	11	01	10	
7	09ea19	78ed29	1dd9e70	04e3d6a	1	0	1	1	1	1	01	10	11	01	
8	13d433	f1da52	3bb3ce0	09c7ad5	0	0	1	1	1	0	10	11	01	10	
9	27a866	e3b4a4	37679c0	138f5aa	1	0	0	1	0	0	01	01	10	01	
10	4f50cd	c76949	2ecf380	271eb55	1	1	1	0	0	0	11	00	01	11	
11	1ea19a	8ed292	1d9e700	4e3d6aa	1	0	0	1	1	1	11	01	10	10	
12	3d4335	1da525	3b3ce00	1c7ad55	1	1	1	1	1	1	11	10	11	01	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	1ac92c	928707	3000275	6aa958d	1	1	1	1	0	1	10	00	01	10	
28	359259	250e0e	20004eb	5552b1a	1	0	0	0	0	0	11	00	10	01	
29	6b24b3	4a1c1d	00009d6	2aa5635	0	1	0	0	0	1	11	01	00	11	
30	564967	94383b	00013ac	554ac6a	1	1	1	0	0	0	10	11	00	01	
31	2c92ce	287077	0002759	2a958d4	0	0	0	0	0	0	11	10	01	10	1
32	59259c	50e0ee	0004eb2	552b1a8	1	0	0	1	0	1	10	01	11	00	0
33	324b39	a1c1dd	0009d65	2a56350	1	1	1	1	0	0	01	10	11	10	0
34	649673	4383ba	0013acb	54ac6a0	1	0	0	1	1	1	10	11	10	01	1
35	492ce7	870774	0027596	2958d40	1	0	0	0	0	0	01	11	11	00	0
36	1259ce	0e0ee8	004eb2d	52b1a81	1	1	1	0	0	1	11	10	11	01	0
37	24b39c	1c1dd1	009d65a	2563502	1	0	0	0	1	1	11	01	11	10	0
38	496738	383ba2	013acb5	4ac6a04	1	0	1	0	1	0	11	11	01	11	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	4627b6	acf367	2a97cbe	785625a	1	0	0	1	1	0	11	01	01	11	1
78	0c4f6d	59e6ce	152f97c	70ac4b5	0	1	1	1	0	1	11	10	10	11	0
79	189eda	b3cd9c	2a5f2f8	615896a	1	1	0	1	1	0	01	11	00	11	0
80	313db5	679b39	14be5f1	42b12d5	0	1	0	1	1	1	11	01	10	10	1
81	627b6b	cf3672	297cbe2	05625aa	0	1	1	0	1	1	10	10	11	01	0
82	44f6d6	9e6ce5	12f97c5	0ac4b54	0	0	1	0	1	0	01	00	11	10	1
83	09edac	3cd9cb	25f2f8a	15896a9	1	1	1	1	1	0	00	01	01	01	1
84	13db59	79b396	0be5f15	2b12d53	1	0	1	1	0	0	10	00	10	11	1
85	27b6b3	f3672d	17cbe2b	5625aa7	1	0	0	0	0	1	11	00	00	11	1
86	4f6d66	e6ce5b	2f97c56	2c4b54f	1	1	1	1	1	0	11	01	00	01	1
87	1edacd	cd9cb6	1f2f8ac	5896a9e	0	0	1	1	0	0	11	10	10	10	1
88	3db59b	9b396d	3e5f159	312d53c	1	0	0	0	1	1	01	11	00	01	
K3	**fd27048ba34cc4**														

Table A-9. Detailed ReadStatus C1-D1 Without Connection State K3

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	31ccc4	3cae8d	165b048	0043f49	1	0	1	1	1	0	01	01	01	01	
Load															
1	639988	795d1b	2cb6091	0087e93	1	0	0	0	1	0	10	10	10	11	
2	473310	f2ba37	196c123	010fd26	0	0	0	1	0	0	01	01	11	10	
3	0e6620	e5746f	32d8246	021fa4c	0	0	1	0	1	0	10	00	11	01	
4	1ccc40	cae8df	25b048d	043f498	1	0	1	1	1	1	01	00	01	11	
5	399881	95d1be	0b6091a	087e931	0	1	0	1	0	1	10	10	00	11	
6	733103	2ba37c	16c1234	10fd262	0	1	0	1	0	1	00	11	00	01	
7	666206	5746f8	2d82469	21fa4c4	1	0	1	0	0	1	00	01	01	00	
8	4cc40d	ae8df0	1b048d2	43f4989	0	1	1	1	0	1	10	10	10	00	
9	19881b	5d1be1	36091a5	07e9312	1	1	0	0	0	1	01	01	00	10	
10	331037	ba37c3	2c1234b	0fd2624	0	0	0	0	1	0	11	10	00	01	
11	66206f	746f86	1824696	1fa4c49	1	1	0	0	0	1	10	01	10	10	
12	4c40de	e8df0d	3048d2d	3f49892	0	1	1	1	0	0	01	11	00	11	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	6f0355	869e73	296877b	4491a11	1	0	0	1	0	0	01	11	00	11	
28	5e06ab	0d3ce6	12d0ef6	0923423	0	1	0	0	1	1	11	01	01	10	
29	3c0d57	1a79cc	25a1dec	1246847	0	1	0	0	0	0	10	11	00	11	
30	781aaf	34f398	0b43bd9	248d08e	1	1	0	1	0	0	00	11	01	10	
31	70355e	69e731	16877b2	491a11c	0	0	0	1	0	0	01	01	11	00	0
32	606abc	d3ce62	2d0ef65	1234238	0	1	1	1	0	1	10	00	11	01	0
33	40d579	a79cc5	1a1deca	2468471	1	0	1	1	1	1	01	00	10	10	0
34	01aaf2	4f398b	343bd95	48d08e2	1	0	0	0	1	0	10	10	01	01	0
35	0355e5	9e7316	2877b2b	11a11c4	1	0	1	0	1	1	01	01	10	11	1
36	06abca	3ce62d	10ef656	2342389	0	0	0	1	0	0	10	11	01	01	0
37	0d5795	79cc5b	21decac	4684712	0	0	1	1	1	0	00	11	11	10	1
38	1aaf2a	f398b6	03bd958	0d08e25	0	1	0	1	1	0	00	01	11	01	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	053515	3e8c7c	275bb51	58142b9	1	0	0	1	1	0	01	00	11	10	1
78	0a6a2b	7d18f9	0eb76a3	3028572	0	0	1	0	1	1	11	00	01	01	1
79	14d457	fa31f2	1d6ed46	6050ae4	0	0	1	0	0	0	01	01	00	10	1
80	29a8af	f463e5	3adda8c	40a15c9	1	1	0	0	1	1	00	11	00	00	1
81	53515e	e8c7cb	35bb518	0142b93	1	1	1	1	1	0	01	10	10	00	1
82	26a2bc	d18f97	2b76a31	0285726	1	0	0	1	1	0	10	11	01	00	0
83	4d4578	a31f2f	16ed462	050ae4d	0	0	1	0	0	0	01	11	10	01	0
84	1a8af0	463e5f	2dda8c5	0a15c9b	1	1	0	0	1	0	00	11	01	11	0
85	3515e0	8c7cbe	1bb518a	142b936	0	1	0	0	1	1	01	10	10	11	0
86	6a2bc0	18f97c	376a315	285726d	0	0	0	1	0	0	10	00	11	01	0
87	545780	31f2f9	2ed462b	50ae4db	0	1	1	1	1	1	00	10	10	11	0
88	28af00	63e5f2	1da8c57	215c9b6	0	0	0	1	0	0	00	01	01	01	
Kp	**03e6205ba71568**														

Table A-10. Detailed ReadStatus C1-D1 Without Connection State Kp

					Taps:		Select:				Shuffle Networks:				
Clock	**LFSR0**	**LFSR1**	**LFSR2**	**LFSR3**	**0**	**2**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**O**
Load	11cd21	13c3ba	165b21f	3fda894	1	0	1	1	1	0	01	01	01	01	
1	239a42	278775	2cb643f	7fb5128	1	0	0	1	1	1	10	10	10	11	
2	473484	4f0eeb	196c87e	7f6a251	0	0	0	0	0	1	01	11	01	01	
3	0e6909	9e1dd7	32d90fd	7ed44a3	1	1	1	0	1	0	10	10	11	00	
4	1cd213	3c3bae	25b21fa	7da8946	1	0	1	0	1	1	11	00	11	01	
5	39a426	78775d	0b643f4	7b5128d	1	1	0	0	0	0	11	01	01	10	
6	73484d	f0eeba	16c87e9	76a251a	1	1	1	1	0	1	11	11	10	00	
7	66909a	e1dd74	2d90fd2	6d44a35	0	0	0	1	1	0	11	11	01	10	
8	4d2134	c3bae8	1b21fa4	5a8946b	0	1	0	1	0	0	10	11	10	01	
9	1a4268	8775d1	3643f49	35128d7	0	0	1	0	0	0	00	11	01	11	
10	3484d0	0eeba2	2c87e93	6a251af	1	0	0	1	0	1	00	10	11	10	
11	6909a1	1dd745	190fd27	544a35e	1	0	0	1	0	0	01	01	10	11	
12	521343	3bae8b	321fa4e	28946bd	1	0	0	1	1	0	11	00	01	11	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	2187ec	4581c9	12775c0	35edca8	1	0	0	1	1	1	01	00	01	10	
28	430fd9	8b0393	24eeb81	6bdb951	0	0	0	0	0	0	11	00	00	11	
29	061fb3	160727	09dd702	57b72a3	0	1	0	0	1	1	10	01	00	10	
30	0c3f67	2c0e4f	13bae05	2f6e547	1	0	0	0	1	1	00	11	00	01	
31	187ece	581c9e	2775c0a	5edca8e	0	0	1	0	1	0	01	10	10	00	0
32	30fd9c	b0393d	0eeb815	3db951c	0	1	1	0	0	1	00	01	11	00	1
33	61fb39	60727b	1dd702b	7b72a38	0	0	1	0	1	1	00	10	10	10	0
34	43f673	c0e4f7	3bae056	76e5470	1	0	1	1	0	1	00	00	11	01	1
35	07ece7	81c9ef	375c0ad	6dca8e0	0	1	1	1	1	0	10	00	10	10	0
36	0fd9cf	0393de	2eb815a	5b951c0	0	0	1	1	1	0	01	00	01	00	0
37	1fb39e	0727bd	1d702b5	372a380	1	0	0	0	1	1	00	10	00	01	1
38	3f673d	0e4f7b	3ae056b	6e54700	0	0	1	0	0	0	01	00	10	00	0
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	3f84e5	b7a87a	371278b	59eab1d	1	1	0	1	1	1	01	01	10	11	0
78	7f09cb	6f50f5	2e24f17	33d563b	1	0	0	0	0	0	11	00	11	01	0
79	7e1396	dea1ea	1c49e2f	67aac77	0	1	0	1	0	1	11	01	10	11	0
80	7c272d	bd43d5	3893c5e	4f558ee	1	0	0	0	1	0	10	10	01	11	1
81	784e5a	7a87aa	31278bc	1eab1dc	0	0	1	1	0	1	01	01	10	11	1
82	709cb5	f50f55	224f179	3d563b9	1	1	0	0	0	0	00	10	01	11	0
83	61396a	ea1eaa	049e2f2	7aac772	0	1	0	0	1	1	01	00	11	10	1
84	4272d4	d43d55	093c5e5	7558ee4	0	1	1	0	1	0	10	00	01	11	0
85	04e5a9	a87aaa	1278bcb	6ab1dc8	0	0	1	0	1	1	01	00	00	11	1
86	09cb53	50f555	24f1797	5563b91	0	0	1	1	1	1	00	01	00	01	1
87	1396a6	a1eaab	09e2f2e	2ac7722	0	1	0	1	0	0	00	00	10	00	1
88	272d4c	43d557	13c5e5c	558ee44	0	1	0	1	0	0	00	00	00	01	
K1	**eb09adb5f6dc25**														

Table A-11. Detailed ReadStatus C1-D1 With Connection State K1

					Taps:		Select:				Shuffle Networks:				
Clock	**LFSR0**	**LFSR1**	**LFSR2**	**LFSR3**	**0**	**2**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**O**
Load	005c25	fd17db	1b2dadb	71cbac2	1	0	1	0	0	0	01	01	01	01	
1	00b84a	fa2fb6	365b5b6	6397584	1	1	0	0	1	0	10	11	10	10	
2	017094	f45f6d	2cb6b6d	472eb09	1	1	1	0	1	1	01	11	11	00	
3	02e128	e8beda	196d6db	0e5d612	1	1	1	1	0	0	10	11	11	10	
4	05c251	d17db4	32dadb7	1cbac25	0	0	1	0	1	1	11	01	11	01	
5	0b84a3	a2fb69	25b5b6f	397584a	0	0	0	1	1	1	01	11	01	10	
6	170947	45f6d3	0b6b6df	72eb094	1	1	0	1	0	1	10	01	10	11	
7	2e128e	8beda7	16d6dbe	65d6129	0	0	0	1	1	0	01	10	01	11	
8	5c251d	17db4f	2dadb7c	4bac253	1	1	0	1	0	1	10	01	00	11	
9	384a3b	2fb69e	1b5b6f9	17584a7	1	0	1	1	1	0	01	10	01	01	
10	709477	5f6d3d	36b6df3	2eb094f	0	0	0	0	1	1	10	11	00	11	
11	6128ef	beda7b	2d6dbe6	5d6129e	0	0	0	1	0	1	00	11	10	01	
12	4251df	7db4f7	1adb7cc	3ac253d	0	1	1	1	1	0	00	01	01	10	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	6fbfeb	7bfe7b	3e64111	29edf22	1	0	0	1	0	1	01	11	00	00	
28	5f7fd6	f7fcf7	3cc8222	53dbe45	0	0	1	1	0	0	11	01	01	00	
29	3effac	eff9ef	3990444	27b7c8a	0	0	1	1	1	1	01	10	11	00	
30	7dff59	dff3de	3320889	4f6f914	0	0	1	1	0	1	00	11	01	10	
31	7bfeb3	bfe7bc	2641112	1edf228	1	1	1	1	0	0	00	01	11	01	1
32	77fd67	7fcf79	0c82224	3dbe451	0	1	1	1	0	1	10	00	11	11	0
33	6ffacf	ff9ef2	1904449	7b7c8a3	0	1	1	1	0	1	01	00	10	11	0
34	5ff59e	ff3de5	3208893	76f9147	1	0	1	0	0	1	00	10	00	11	1
35	3feb3c	fe7bcb	2411127	6df228f	0	1	1	0	1	1	10	00	01	01	0
36	7fd679	fcf796	082224e	5be451f	0	1	1	1	0	1	01	00	00	10	1
37	7facf2	f9ef2c	104449d	37c8a3f	1	0	0	1	0	0	00	10	00	01	0
38	7f59e5	f3de58	208893a	6f9147f	0	0	1	1	0	0	01	01	00	10	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	2842c9	33550f	053e990	7fcbce1	0	1	1	0	1	0	01	11	10	01	1
78	508593	66aa1e	0a7d321	7f979c3	1	0	0	1	1	0	00	11	11	10	1
79	210b27	cd543d	14fa642	7f2f386	1	0	0	0	1	1	01	01	11	01	1
80	42164f	9aa87b	29f4c84	7e5e70d	1	0	0	1	1	0	11	10	01	10	1
81	042c9f	3550f7	13e9909	7cbce1b	1	1	0	0	0	1	11	11	00	01	0
82	08593f	6aa1ee	27d3212	7979c37	1	0	1	1	1	1	11	11	01	00	0
83	10b27e	d543dd	0fa6424	72f386f	1	0	0	0	0	1	11	11	10	10	0
84	2164fc	aa87ba	1f4c849	65e70df	0	0	1	1	0	1	11	11	01	11	1
85	42c9f9	550f75	3e99093	4bce1be	0	1	1	0	1	0	01	11	11	01	1
86	0593f3	aa1eeb	3d32127	179c37c	0	0	0	0	1	0	00	11	11	11	1
87	0b27e7	543dd6	3a6424f	2f386f8	0	1	0	0	0	1	00	10	11	11	0
88	164fcf	a87bad	34c849f	5e70df0	1	1	1	0	0	1	00	00	11	11	
K2	**71ebb3cc7693d4**														

Table A-12. Detailed ReadStatus C1-D1 With Connection State K2

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	0b13d4	0cf1da	1c3bb3c	1b09c7a	1	0	0	1	1	0	01	01	01	01	
Load															
1	1627a8	19e3b4	3877679	36138f5	0	1	0	1	1	0	11	00	10	11	
2	2c4f50	33c769	30eecf3	6c271eb	1	0	1	1	0	1	10	10	01	10	
3	589ea1	678ed2	21dd9e7	584e3d6	0	1	0	1	1	0	11	01	10	01	
4	313d43	cf1da5	03bb3ce	309c7ad	1	1	0	0	1	0	10	10	11	10	
5	627a86	9e3b4a	077679c	6138f5a	1	1	1	0	1	1	01	01	11	01	
6	44f50c	3c7694	0eecf38	4271eb5	0	0	1	0	0	1	10	11	01	10	
7	09ea19	78ed29	1dd9e70	04e3d6a	1	0	1	1	1	1	01	10	11	01	
8	13d433	f1da52	3bb3ce0	09c7ad5	0	0	1	1	1	0	10	11	01	10	
9	27a866	e3b4a4	37679c0	138f5aa	1	0	0	1	0	0	01	01	10	01	
10	4f50cd	c76949	2ecf380	271eb55	1	1	1	0	0	0	11	00	01	11	
11	1ea19a	8ed292	1d9e700	4e3d6aa	1	0	0	1	1	1	11	01	10	10	
12	3d4335	1da525	3b3ce00	1c7ad55	1	1	1	1	1	1	11	10	11	01	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	1ac92c	928707	3000275	6aa958d	1	1	1	1	0	1	10	00	01	10	
28	359259	250e0e	20004eb	5552b1a	1	0	0	0	0	0	11	00	10	01	
29	6b24b3	4a1c1d	00009d6	2aa5635	0	1	0	0	0	1	11	01	00	11	
30	564967	94383b	00013ac	554ac6a	1	1	1	0	0	0	10	11	00	01	
31	2c92ce	287077	0002759	2a958d4	0	0	0	0	0	0	11	10	01	10	1
32	59259c	50e0ee	0004eb2	552b1a8	1	0	0	1	0	1	10	01	11	00	0
33	324b39	a1c1dd	0009d65	2a56350	1	1	1	1	0	0	01	10	11	10	0
34	649673	4383ba	0013acb	54ac6a0	1	0	0	1	1	1	10	11	10	01	1
35	492ce7	870774	0027596	2958d40	1	0	0	0	0	0	01	11	11	00	0
36	1259ce	0e0ee8	004eb2d	52b1a81	1	1	1	0	0	1	11	10	11	01	0
37	24b39c	1c1dd1	009d65a	2563502	1	0	0	0	1	1	11	01	11	10	0
38	496738	383ba2	013acb5	4ac6a04	1	0	1	0	1	0	11	11	01	11	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	4627b6	acf367	2a97cbe	785625a	1	0	0	1	1	0	11	01	01	11	1
78	0c4f6d	59e6ce	152f97c	70ac4b5	0	1	1	1	0	1	11	10	10	11	0
79	189eda	b3cd9c	2a5f2f8	615896a	1	1	0	1	1	0	01	11	00	11	0
80	313db5	679b39	14be5f1	42b12d5	0	1	0	1	1	1	11	01	10	10	1
81	627b6b	cf3672	297cbe2	05625aa	0	1	1	0	1	1	10	10	11	01	0
82	44f6d6	9e6ce5	12f97c5	0ac4b54	0	0	1	0	1	0	01	00	11	10	1
83	09edac	3cd9cb	25f2f8a	15896a9	1	1	1	1	1	0	00	01	01	01	1
84	13db59	79b396	0be5f15	2b12d53	1	0	1	1	0	0	10	00	10	11	1
85	27b6b3	f3672d	17cbe2b	5625aa7	1	0	0	0	0	1	11	00	00	11	1
86	4f6d66	e6ce5b	2f97c56	2c4b54f	1	1	1	1	1	0	11	01	00	01	1
87	1edacd	cd9cb6	1f2f8ac	5896a9e	0	0	1	1	0	0	11	10	10	10	1
88	3db59b	9b396d	3e5f159	312d53c	1	0	0	0	1	1	01	11	00	01	
K3	**fd27048ba34cc4**														

Table A-13. Detailed ReadStatus C1-D1 With Connection State K3

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
LLoad	31ccc4	3cae8d	165b048	0843f49	1	0	1	1	1	0	01	01	01	01	
1	639988	795d1b	2cb6091	1087e92	1	0	0	0	1	0	10	10	10	11	
2	473310	f2ba37	196c123	210fd24	0	0	0	1	0	0	01	01	11	10	
3	0e6620	e5746f	32d8246	421fa48	0	1	1	0	1	0	10	00	11	01	
4	1ccc40	cae8df	25b048d	043f491	1	0	1	1	1	1	01	00	01	11	
5	399881	95d1be	0b6091a	087e923	0	1	0	1	0	1	10	10	00	11	
6	733103	2ba37c	16c1234	10fd246	0	1	0	1	0	1	00	11	00	01	
7	666206	5746f8	2d82469	21fa48c	1	0	1	0	0	1	00	01	01	00	
8	4cc40d	ae8df0	1b048d2	43f4919	0	1	1	1	0	1	10	10	10	00	
9	19881b	5d1be1	36091a5	07e9233	0	1	0	0	0	1	01	01	00	10	
10	331037	ba37c3	2c1234b	0fd2466	0	0	0	0	1	0	10	10	00	01	
11	66206f	746f86	1824696	1fa48cd	1	1	0	0	0	1	00	01	10	10	
12	4c40de	e8df0d	3048d2d	3f4919b	1	1	1	1	0	0	01	10	00	11	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	6f0355	869e73	296877b	0cdb8f4	1	1	0	1	0	0	00	01	00	10	
28	5e06ab	0d3ce6	12d0ef6	19b71e8	1	1	0	0	1	1	01	00	01	00	
29	3c0d57	1a79cc	25a1dec	336e3d1	1	1	0	0	0	1	11	00	00	10	
30	781aaf	34f398	0b43bd9	66dc7a2	0	0	0	1	0	0	11	01	00	01	
31	70355e	69e731	16877b2	4db8f45	0	0	0	1	0	1	10	10	01	10	0
32	606abc	d3ce62	2d0ef65	1b71e8a	0	1	1	1	0	1	00	11	10	01	0
33	40d579	a79cc5	1a1deca	36e3d15	0	0	1	1	1	1	00	01	01	10	0
34	01aaf2	4f398b	343bd95	6dc7a2b	1	0	0	0	1	0	00	00	10	11	1
35	0355e5	9e7316	2877b2b	5b8f456	0	1	1	0	1	0	01	00	01	10	0
36	06abca	3ce62d	10ef656	371e8ac	1	0	0	1	0	0	00	01	00	01	0
37	0d5795	79cc5b	21decac	6e3d159	0	0	1	1	1	1	01	00	01	10	0
38	1aaf2a	f398b6	03bd958	5c7a2b2	0	0	0	1	1	1	00	10	00	11	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	053515	3e8c7c	275bb51	7ba8363	0	0	0	1	1	1	11	00	01	00	0
78	0a6a2b	7d18f9	0eb76a3	77506c7	1	1	1	0	1	0	10	10	00	10	0
79	14d457	fa31f2	1d6ed46	6ea0d8e	1	0	1	0	0	1	11	00	10	00	0
80	29a8af	f463e5	3adda8c	5d41b1d	1	1	0	0	1	0	11	01	00	10	0
81	53515e	e8c7cb	35bb518	3a8363a	0	1	1	1	1	0	11	11	00	00	1
82	26a2bc	d18f97	2b76a31	7506c74	0	1	0	1	1	0	01	11	10	00	1
83	4d4578	a31f2f	16ed462	6a0d8e8	0	1	1	0	0	0	10	01	11	00	1
84	1a8af0	463e5f	2dda8c5	541b1d0	0	0	0	0	1	0	01	10	10	01	0
85	3515e0	8c7cbe	1bb518a	28363a0	0	1	0	0	1	1	10	00	11	10	1
86	6a2bc0	18f97c	376a315	506c741	1	1	0	1	0	1	00	01	01	11	0
87	545780	31f2f9	2ed462b	20d8e83	0	0	1	1	1	0	01	00	11	01	0
88	28af00	63e5f2	1da8c57	41b1d06	0	1	0	1	0	1	00	10	01	11	
K4	**2e02408cb8cf44**														

Table A-14. Detailed ReadStatus C1-D1 With Connection State K4

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	004f44	0032e3	0202408	0000b80	0	0	1	0	0	0	01	01	01	01	
Load															
1	009e88	0065c7	0404810	0001701	1	0	0	0	0	0	00	11	10	10	
2	013d10	00cb8e	0809021	0002e03	1	0	0	1	0	0	01	10	01	01	
3	027a20	01971d	1012042	0005c06	0	0	1	1	1	0	11	01	10	10	
4	04f440	032e3b	2024084	000b80d	0	1	1	0	0	0	01	10	11	00	
5	09e881	065c77	0048108	001701b	0	0	1	0	0	0	00	01	11	01	
6	13d103	0cb8ee	0090210	002e036	1	0	1	1	1	1	00	10	10	11	
7	27a206	1971dc	0120420	005c06c	1	0	0	0	0	0	10	01	01	01	
8	4f440d	32e3b9	0240841	00b80d9	1	1	1	1	0	1	01	11	10	10	
9	1e881a	65c772	0481083	01701b2	1	0	0	1	0	1	10	11	01	11	
10	3d1035	cb8ee4	0902106	02e0365	1	1	0	1	0	1	01	11	11	01	
11	7a206a	971dc8	120420c	05c06ca	1	0	0	0	0	0	11	01	11	10	
12	7440d5	2e3b90	2408419	0b80d94	1	0	1	0	0	0	11	11	10	01	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	6aee4c	c87d45	20cb075	6ca48cf	0	0	1	0	0	1	11	11	01	01	
28	55dc98	90fa8b	01960eb	594919f	1	1	1	1	1	0	01	11	11	00	
29	2bb931	21f516	032c1d6	329233f	0	0	0	1	0	0	10	11	11	01	
30	577263	43ea2d	06583ad	652467f	1	0	1	1	1	1	00	11	11	11	
31	2ee4c6	87d45b	0cb075a	4a48cfe	0	0	1	1	1	0	10	01	11	11	1
32	5dc98c	0fa8b7	1960eb4	14919fd	1	1	1	1	0	0	01	00	11	11	0
33	3b9319	1f516e	32c1d69	29233fb	0	1	0	0	0	1	10	10	10	11	0
34	772633	3ea2dd	2583ad2	52467f6	0	1	0	1	0	0	00	01	01	11	0
35	6e4c66	7d45bb	0b075a4	248cfec	1	1	1	0	0	0	00	00	11	10	0
36	5c98cc	fa8b77	160eb48	4919fd9	1	1	0	1	0	0	10	00	10	01	1
37	393198	f516ef	2c1d691	1233fb2	1	0	0	0	1	1	01	10	00	11	1
38	726330	ea2dde	183ad22	2467f65	1	0	1	0	1	1	11	00	10	01	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	6b4631	09c22a	08d49ca	4e03385	0	0	1	1	1	0	01	01	10	00	0
78	568c63	138455	11a9395	1c0670a	0	1	0	1	0	0	00	10	11	00	1
79	2d18c6	2708ab	235272a	380ce15	1	1	0	0	1	0	00	01	10	01	1
80	5a318c	4e1157	06a4e55	7019c2b	1	0	0	0	0	0	01	10	01	10	1
81	346319	9c22ae	0d49caa	6033857	1	0	1	0	0	1	11	00	11	00	0
82	68c633	38455c	1a93955	40670af	1	0	1	0	1	1	11	01	10	10	0
83	518c66	708ab8	35272ab	00ce15f	0	0	0	1	0	0	11	11	01	01	0
84	2318cc	e11570	2a4e557	019c2be	0	0	0	0	0	0	10	11	11	10	1
85	463199	c22ae0	149caae	033857d	1	0	0	0	1	1	00	11	11	01	1
86	0c6332	8455c1	293955c	0670afa	0	0	1	0	1	1	01	10	11	10	0
87	18c665	08ab82	1272ab8	0ce15f4	0	0	1	1	1	1	00	01	11	11	1
88	318ccb	115704	24e5571	19c2be9	1	1	0	0	0	0	00	00	11	11	
Kp	**b1c0a2a4d66570**														

Table A-15. Detailed ReadStatus C1-D1 With Connection State Kp

					Taps:		Select:				Shuffle Networks:				
Clock	**LFSR0**	**LFSR1**	**LFSR2**	**LFSR3**	**0**	**2**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**O**
Load	5bd0d1	455d1a	0454f87	19d4a64	0	1	1	0	1	0	01	01	01	01	
1	37a1a3	8aba34	08a9f0e	33a94c9	0	1	0	1	0	1	00	11	00	11	
2	6f4347	157468	1153e1c	6752993	1	0	1	0	1	0	00	01	01	01	
3	5e868f	2ae8d1	22a7c39	4ea5326	1	1	0	1	0	1	10	10	00	11	
4	3d0d1f	55d1a3	054f872	1d4a64d	1	0	0	1	0	0	01	11	00	01	
5	7a1a3f	aba347	0a9f0e5	3a94c9a	0	0	0	1	1	0	11	01	01	10	
6	74347e	57468f	153e1ca	7529935	1	0	0	0	1	1	10	10	10	01	
7	6868fc	ae8d1f	2a7c394	6a5326b	0	0	1	1	1	0	01	01	11	00	
8	50d1f8	5d1a3e	14f8728	54a64d6	0	0	1	0	1	1	00	10	11	01	
9	21a3f0	ba347c	29f0e50	294c9ac	0	0	0	0	1	0	00	00	11	10	
10	4347e1	7468f9	13e1ca1	5299359	1	0	1	0	0	0	00	00	01	01	
11	068fc3	e8d1f3	27c3943	25326b3	1	0	0	1	0	1	10	00	10	10	
12	0d1f87	d1a3e6	0f87287	4a64d67	1	0	0	1	0	1	01	10	00	11	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	43f803	f347b1	143cc5b	6b39527	0	1	1	0	1	1	11	01	00	00	
28	07f007	e68f62	28798b6	5672a4f	0	1	1	1	1	1	01	11	00	00	
29	0fe00f	cd1ec4	10f316c	2ce549e	0	1	1	0	1	1	00	11	10	00	
30	1fc01e	9a3d89	21e62d9	59ca93d	0	1	1	0	0	0	00	10	11	00	
31	3f803c	347b12	03cc5b2	339527b	1	0	0	0	0	0	00	00	11	01	0
32	7f0079	68f625	0798b64	672a4f7	1	0	0	1	1	1	01	00	10	11	1
33	7e00f3	d1ec4a	0f316c8	4e549ef	0	1	0	1	1	0	11	00	01	01	1
34	7c01e7	a3d894	1e62d91	1ca93de	0	0	0	1	0	1	10	10	00	11	1
35	7803ce	47b128	3cc5b22	39527bd	1	0	0	1	0	0	00	11	00	01	0
36	70079d	8f6250	398b644	72a4f7a	0	0	0	0	0	1	01	01	01	10	0
37	600f3a	1ec4a1	3316c89	6549ef5	1	1	0	1	1	0	10	10	10	01	1
38	401e74	3d8942	262d912	4a93dea	0	1	0	1	0	0	01	11	01	10	0
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	7f8f7f	bbfd7e	12cffe2	4ddf626	1	1	0	1	0	0	01	10	11	11	0
78	7f1efe	77fafd	259ffc5	1bbec4d	1	0	0	1	1	1	11	01	10	11	1
79	7e3dfc	eff5fb	0b3ff8b	377d89b	1	0	0	1	1	1	11	10	11	01	1
80	7c7bf9	dfebf6	167ff16	6efb136	0	1	1	1	1	1	11	11	01	10	1
81	78f7f3	bfd7ec	2cffe2c	5df626c	0	0	1	1	1	1	01	11	10	11	1
82	71efe7	7fafd9	19ffc59	3bec4d8	0	1	1	1	1	1	00	11	11	01	0
83	63dfcf	ff5fb3	33ff8b3	77d89b1	1	0	1	0	1	0	00	01	11	10	1
84	47bf9e	febf66	27ff167	6fb1362	1	0	0	1	1	1	10	10	01	01	1
85	0f7f3c	fd7ecc	0ffe2ce	5f626c5	1	0	1	0	1	1	01	11	00	10	0
86	1efe78	fafd99	1ffc59c	3ec4d8a	1	1	1	1	1	0	10	11	10	01	1
87	3dfcf0	f5fb32	3ff8b38	7d89b14	1	1	1	1	1	0	11	01	11	10	0
88	7bf9e0	ebf664	3ff1670	7b13628	1	0	1	1	1	0	11	10	11	01	
K5	**5bc1db127f1e27**														

Table A-16. Detailed ReadM C1-D1 K5

					Taps:		Select:				Shuffle Networks:				
Clock	**LFSR0**	**LFSR1**	**LFSR2**	**LFSR3**	**0**	**2**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**O**
Load	5813ad	333e3c	1bb5893	020383b	1	1	0	0	1	0	01	01	01	01	
1	30275a	667c78	376b126	0407077	1	1	0	0	0	0	11	10	00	11	
2	604eb5	ccf8f1	2ed624d	080e0ef	0	1	1	1	1	0	11	01	01	10	
3	409d6b	99f1e3	1dac49b	101c1de	0	0	0	1	0	0	01	10	10	01	
4	013ad7	33e3c6	3b58936	20383bc	0	1	0	1	1	1	10	01	00	11	
5	0275af	67c78d	36b126c	4070778	1	0	1	1	1	1	00	10	10	01	
6	04eb5e	cf8f1a	2d624d9	00e0ef0	0	0	1	1	0	1	10	01	01	00	
7	09d6bd	9f1e35	1ac49b2	01c1de1	1	1	1	0	0	0	01	00	11	00	
8	13ad7b	3e3c6a	3589365	0383bc3	0	1	0	0	0	0	10	01	10	01	
9	275af6	7c78d4	2b126ca	0707787	1	1	1	0	1	0	00	11	00	11	
10	4eb5ec	f8f1a9	1624d94	0e0ef0f	0	0	0	1	0	0	10	10	10	10	
11	1d6bd9	f1e353	2c49b29	1c1de1f	0	0	1	1	0	0	00	11	00	01	
12	3ad7b3	e3c6a7	1893653	383bc3f	0	1	1	1	1	1	00	01	01	10	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	59b030	53f86c	329b3a1	61ff712	0	1	0	1	1	1	01	10	10	00	
28	336060	a7f0d8	2536742	43fee24	0	1	1	1	1	1	10	01	01	00	
29	66c0c1	4fe1b0	0a6ce84	07fdc49	0	1	1	1	0	1	01	00	10	10	
30	4d8182	9fc360	14d9d08	0ffb893	0	0	0	1	1	1	00	10	00	11	
31	1b0304	3f86c1	29b3a10	1ff7127	0	1	0	1	1	1	00	01	00	01	0
32	360608	7f0d82	1367421	3fee24e	1	0	0	0	0	1	00	00	10	00	0
33	6c0c10	fe1b04	26ce842	7fdc49c	0	0	0	0	0	0	01	00	00	10	1
34	581821	fc3608	0d9d084	7fb8939	1	1	0	0	1	1	10	00	00	00	1
35	303042	f86c10	1b3a109	7f71272	1	0	0	0	1	1	01	01	00	00	0
36	606084	f0d821	3674213	7ee24e5	1	0	1	1	1	1	11	10	00	00	0
37	40c109	e1b042	2ce8426	7dc49cb	1	0	1	1	0	0	11	11	00	00	0
38	018213	c36085	19d084d	7b89396	0	0	0	0	1	0	11	11	01	00	0
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
85	04faad	34d779	00c170e	5ceebf5	1	1	1	1	0	1	10	01	10	01	0
86	09f55b	69aef3	0182e1c	39dd7eb	0	0	1	1	0	0	11	00	01	10	1
87	13eab7	d35de7	0305c39	73bafd7	1	0	1	0	0	1	01	10	10	00	0
88	27d56f	a6bbce	060b872	6775fae	0	0	1	1	0	1	10	01	01	10	0
89	4faadf	4d779d	0c170e4	4eebf5d	1	0	0	0	1	1	01	00	11	01	1
90	1f55be	9aef3a	182e1c9	1dd7ebb	0	1	1	1	0	0	11	00	01	10	0
91	3eab7d	35de75	305c393	3bafd77	0	1	0	1	1	1	01	10	10	00	1
92	7d56fb	6bbceb	20b8727	775faef	1	1	1	1	1	0	10	01	01	00	1
93	7aadf7	d779d7	0170e4e	6ebf5df	1	1	0	0	1	1	11	00	10	01	0
94	755bee	aef3af	02e1c9c	5d7ebbf	1	1	1	1	0	1	11	01	01	00	1
95	6ab7dc	5de75e	05c3939	3afd77f	1	1	0	1	0	1	11	10	11	00	1
96	556fb8	bbcebc	0b87272	75faeff	0	1	1	1	0	1	11	11	10	10	
Ke	**da4245977574bf86**														

Table A-17. Detailed ReadM C1-D1 Ke

					Taps:		Select:				Shuffle Networks:				
Clock	**LFSR0**	**LFSR1**	**LFSR2**	**LFSR3**	**0**	**2**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**O**
Load	1fd0d1	065d1a	39a0f87	4da8a64	0	0	1	0	0	1	01	01	01	01	
1	3fa1a2	0cba35	3341f0e	1b514c9	0	1	0	1	0	0	00	11	10	00	
2	7f4344	19746a	2683e1c	36a2993	1	0	1	0	0	1	00	01	01	01	
3	7e8689	32e8d5	0d07c39	6d45327	1	0	0	1	0	0	10	10	10	00	
4	7d0d13	65d1aa	1a0f873	5a8a64e	1	0	0	1	0	0	01	11	00	01	
5	7a1a26	cba354	341f0e6	3514c9c	0	1	0	1	1	0	11	01	01	10	
6	74344c	9746a9	283e1cc	6a29939	1	0	0	0	1	1	10	10	10	01	
7	686899	2e8d52	107c398	5453273	0	0	1	1	1	0	01	01	11	00	
8	50d133	5d1aa4	20f8731	28a64e7	0	0	1	0	1	1	00	10	11	01	
9	21a266	ba3548	01f0e62	514c9ce	1	0	0	0	1	0	00	00	11	10	
10	4344cc	746a91	03e1cc4	229939d	1	1	1	0	0	0	01	00	01	01	
11	068999	e8d523	07c3989	453273b	1	0	0	1	0	1	10	01	10	10	
12	0d1333	d1aa47	0f87313	0a64e77	1	1	0	1	0	1	01	10	01	11	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	19de19	23c0ca	1898b1f	73bd1e8	1	1	1	1	1	1	11	00	11	10	
28	33bc33	478194	313163f	677a3d1	0	0	0	1	1	1	11	10	01	11	
29	677867	8f0329	2262c7e	4ef47a2	1	0	1	0	0	1	10	11	00	11	
30	4ef0cf	1e0653	04c58fd	1de8f44	0	1	1	0	0	1	11	10	01	01	
31	1de19f	3c0ca6	098b1fa	3bd1e88	1	0	1	0	0	0	01	01	11	00	0
32	3bc33f	78194d	13163f5	77a3d11	0	1	1	0	1	1	10	11	10	01	0
33	77867e	f0329a	262c7ea	6f47a23	0	0	0	0	0	0	01	10	11	00	0
34	6f0cfd	e06534	0c58fd5	5e8f446	0	1	0	0	1	0	10	00	11	01	1
35	5e19fa	c0ca68	18b1fab	3d1e88d	0	0	0	1	1	0	00	01	01	11	1
36	3c33f5	8194d1	3163f57	7a3d11a	0	1	0	1	0	1	00	00	10	11	0
37	7867eb	0329a2	22c7eaf	747a234	0	1	1	0	0	1	00	00	00	11	0
38	70cfd6	065344	058fd5e	68f4468	0	0	1	0	0	1	00	00	00	01	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	4e7d3e	a84605	01c6490	04e1ec0	0	0	1	0	0	1	10	10	00	10	0
78	1cfa7d	508c0a	038c920	09c3d80	0	0	1	1	0	0	01	00	01	01	0
79	39f4fa	a11815	0719240	1387b00	0	1	1	0	1	0	00	10	10	10	0
80	73e9f5	42302b	0e32481	270f600	1	1	1	0	1	0	00	00	11	00	1
81	67d3eb	846056	1c64903	4e1ec00	0	1	1	0	0	0	10	00	01	01	1
82	4fa7d6	08c0ad	38c9206	1c3d801	0	0	0	1	0	1	01	00	10	10	0
83	1f4fac	11815a	319240d	387b003	1	1	1	1	1	1	10	00	00	11	0
84	3e9f58	2302b4	232481b	70f6007	1	0	0	0	0	1	11	00	00	01	1
85	7d3eb0	460568	0649036	61ec00e	1	0	0	0	0	1	11	01	00	00	0
86	7a7d60	8c0ad0	0c9206d	43d801c	1	1	1	0	1	0	11	11	00	00	1
87	74fac1	1815a1	19240db	07b0039	0	1	1	0	0	1	11	11	10	00	1
88	69f583	302b43	32481b7	0f60072	0	0	1	0	0	1	01	11	01	10	
K6	**d307089a5e014c**														

Table A-18. Detailed ReadZ C1-D1 K6

					Taps:		Select:				Shuffle Networks:				
Clock	**LFSR0**	**LFSR1**	**LFSR2**	**LFSR3**	**0**	**2**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**O**
Load	202669	27fc02	038c4d2	02020e1	0	0	0	1	0	0	01	01	01	01	
1	404cd3	4ff804	07189a4	04041c3	1	1	1	1	1	0	10	00	11	10	
2	0099a6	9ff008	0e31349	0808387	1	1	0	1	1	0	11	00	01	01	
3	01334c	3fe010	1c62692	101070e	1	0	0	1	0	0	11	10	00	11	
4	026699	7fc021	38c4d25	2020e1d	0	1	1	1	0	1	11	11	00	10	
5	04cd32	ff8042	3189a4b	4041c3a	0	1	1	1	0	0	01	11	01	01	
6	099a64	ff0084	2313496	0083874	1	0	0	0	1	0	00	11	11	10	
7	1334c8	fe0109	062692c	01070e9	0	1	0	0	0	0	01	10	11	01	
8	266990	fc0213	0c4d258	020e1d3	0	1	1	0	0	0	10	00	11	11	
9	4cd320	f80427	189a4b0	041c3a7	1	0	1	0	1	0	01	00	10	11	
10	19a641	f0084e	3134961	083874e	0	0	0	0	1	1	10	01	01	10	
11	334c82	e0109d	22692c2	1070e9c	0	0	1	0	0	1	00	11	00	11	
12	669905	c0213b	04d2585	20e1d38	0	0	0	0	1	1	00	10	01	01	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	029dc3	9dbade	2c2ab35	69c7046	1	1	0	1	0	0	00	10	01	10	
28	053b87	3b75bd	185566a	538e08c	0	1	0	0	1	0	01	01	10	00	
29	0a770e	76eb7b	30aacd5	271c119	1	1	1	1	0	0	10	10	01	00	
30	14ee1c	edd6f7	21559aa	4e38232	0	1	1	1	1	1	11	01	10	00	
31	29dc38	dbadef	02ab354	1c70465	0	1	1	1	0	1	01	10	11	00	1
32	53b870	b75bdf	05566a9	38e08ca	1	0	0	0	1	1	00	11	10	10	0
33	2770e0	6eb7bf	0aacd53	71c1194	0	1	1	1	0	0	01	10	11	01	1
34	4ee1c1	dd6f7f	1559aa7	6382328	0	1	1	0	1	0	00	11	10	11	0
35	1dc382	badeff	2ab354f	4704650	1	1	1	1	1	0	00	10	11	10	0
36	3b8705	75bdff	1566a9e	0e08ca0	1	0	0	1	0	0	10	01	01	01	0
37	770e0b	eb7bff	2acd53d	1c11940	1	1	0	0	0	0	01	10	11	10	0
38	6e1c16	d6f7ff	159aa7a	3823281	1	0	0	1	1	1	11	00	11	01	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
85	62b08f	7afe04	1c4008d	18d917f	0	1	0	1	0	0	00	11	01	00	1
86	45611e	f5fc08	388011a	31b22ff	1	1	1	1	0	1	00	01	11	00	1
87	0ac23c	ebf811	3100235	63645ff	1	1	1	1	0	1	10	00	11	10	1
88	158479	d7f023	220046b	46c8bff	1	1	0	1	0	0	11	00	10	11	0
89	2b08f2	afe046	04008d7	0d917fe	0	1	0	1	0	0	11	10	00	11	0
90	5611e5	5fc08c	08011af	1b22ffd	0	1	0	1	0	1	10	11	00	10	1
91	2c23cb	bf8118	100235f	3645ffb	1	1	0	1	0	0	00	11	01	01	1
92	584796	7f0231	20046be	6c8bff6	0	1	1	0	0	0	01	01	11	10	0
93	308f2d	fe0463	0008d7d	5917fec	0	0	0	0	0	0	00	11	10	01	0
94	611e5a	fc08c6	0011afb	322ffd8	0	0	0	0	1	1	00	10	01	11	1
95	423cb4	f8118d	00235f6	645ffb0	0	1	0	0	0	0	00	00	10	11	0
96	047969	f0231a	0046bec	48bff60	0	0	1	0	0	1	00	00	00	11	
Kz	**4cf99e93e03bfbc2**														

Table A-19. Detailed ReadZ C1-D1 Kz

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	45ed5d	cc57cf	21bd305	0530789	1	1	1	0	1	1	01	01	01	01	
1	0bdaba	98af9f	037a60b	0a60f13	1	1	1	1	1	1	10	11	00	10	
2	17b574	315f3e	06f4c17	14c1e27	0	0	0	0	1	0	11	01	10	01	
3	2f6ae9	62be7c	0de982e	2983c4f	1	0	1	1	0	0	10	11	01	10	
4	5ed5d3	c57cf8	1bd305d	530789f	0	1	1	0	1	0	11	01	11	00	
5	3daba6	8af9f1	37a60ba	260f13e	1	0	0	1	0	0	01	11	01	01	
6	7b574d	15f3e2	2f4c175	4c1e27d	0	1	1	1	0	0	11	01	11	10	
7	76ae9b	2be7c4	1e982eb	183c4fb	0	1	0	1	1	1	01	10	11	01	
8	6d5d37	57cf88	3d305d6	30789f7	1	0	1	1	1	1	10	01	01	10	
9	5aba6f	af9f11	3a60bac	60f13ee	0	0	0	1	0	1	11	00	10	11	
10	3574df	5f3e23	34c1758	41e27dc	1	0	1	0	0	1	10	10	00	11	
11	6ae9be	be7c46	2982eb0	03c4fb9	0	1	1	0	0	0	11	00	01	01	
12	55d37c	7cf88d	1305d61	0789f72	1	1	1	1	0	0	01	01	10	10	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	3e2eb9	46bf44	2b09b09	7b93a94	0	0	0	1	0	0	01	00	10	00	
28	7c5d73	8d7e88	1613612	7727528	0	1	1	0	1	1	10	00	00	01	
29	78bae7	1afd11	2c26c25	6e4ea51	1	1	0	1	0	0	01	00	00	00	
30	7175cf	35fa23	184d84b	5c9d4a2	1	0	1	1	0	0	11	00	00	00	
31	62eb9e	6bf447	309b096	393a945	0	0	1	1	1	1	11	10	00	00	0
32	45d73c	d7e88f	213612c	727528b	0	0	1	1	1	1	01	11	00	00	0
33	0bae78	afd11e	026c259	64ea516	1	0	0	1	0	1	00	11	10	00	0
34	175cf0	5fa23c	04d84b2	49d4a2d	1	1	1	1	1	0	01	01	01	10	0
35	2eb9e0	bf4478	09b0964	13a945a	0	1	0	0	1	1	10	10	10	01	0
36	5d73c1	7e88f0	13612c8	27528b4	0	1	1	1	0	0	00	01	11	00	1
37	3ae783	fd11e1	26c2590	4ea5169	0	1	1	0	0	1	00	00	11	01	0
38	75cf07	fa23c3	0d84b21	1d4a2d3	0	0	1	0	0	0	00	00	10	10	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	609be1	c52fae	3a98711	404483c	1	0	0	0	1	0	10	10	10	11	1
78	4137c3	8a5f5d	3530e23	0089079	1	1	0	0	1	0	01	01	11	10	0
79	026f86	14beba	2a61c46	01120f3	0	1	1	1	0	0	11	10	01	01	1
80	04df0c	297d75	14c388d	02241e7	1	0	1	0	0	1	01	11	10	10	0
81	09be19	52faea	298711b	04483cf	1	1	0	1	0	0	10	11	01	11	0
82	137c33	a5f5d5	130e236	089079f	0	1	1	1	0	0	01	11	11	10	0
83	26f866	4bebab	261c46d	1120f3f	0	1	1	1	1	1	00	11	11	01	0
84	4df0cd	97d757	0c388db	2241e7f	1	0	1	1	1	0	00	01	11	10	1
85	1be19b	2faeaf	18711b6	4483cff	1	1	1	1	1	0	10	00	11	01	1
86	37c337	5f5d5f	30e236c	09079ff	0	1	1	0	0	0	11	00	01	11	0
87	6f866f	bebabf	21c46d8	120f3fc	0	1	0	1	0	0	01	01	10	10	0
88	5f0cde	7d757f	0388db1	241e7fc	1	1	0	0	0	0	10	00	01	01	
K7	**30bbb798f87e50**														

Table A-20. Detailed ReadZ C1-D1 K7

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	1fe818	0270fc	3ba3cc7	4da9776	0	0	1	0	0	1	01	01	01	01	
1	3fd031	04e1f9	374798e	1b52eec	0	1	1	1	0	0	00	11	10	00	
2	7fa063	09c3f2	2e8f31d	36a5dd8	1	0	0	1	0	1	00	01	01	01	
3	7f40c6	1387e4	1d1e63b	6d4bbb0	1	0	1	1	1	0	01	00	11	00	
4	7e818c	270fc8	3a3cc76	5a97761	1	1	0	0	1	0	10	10	01	01	
5	7d0318	4e1f91	34798ec	352eec2	1	0	0	0	1	1	01	01	10	11	
6	7a0631	9c3f22	28f31d9	6a5dd84	0	0	0	0	1	0	11	10	01	01	
7	740c63	387e44	11e63b3	54bbb09	0	0	0	0	0	1	10	01	10	11	
8	6818c7	70fc88	23cc767	2977613	1	0	0	1	0	1	00	11	00	11	
9	50318f	e1f910	0798ece	52eec26	1	1	0	1	1	1	01	01	01	01	
10	20631e	c3f220	0f31d9d	25dd84d	1	1	1	1	1	0	11	00	10	10	
11	40c63d	87e440	1e63b3a	4bbb09b	1	1	1	1	0	1	11	10	01	00	
12	018c7b	0fc880	3cc7675	1776136	0	1	0	1	0	1	11	11	10	00	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	3dc1e9	404047	33ac42b	09b36e0	1	1	1	0	0	1	00	01	11	11	
28	7b83d2	80808f	2758857	1366dc1	1	1	0	1	1	1	10	10	10	11	
29	7707a4	01011f	0eb10af	26cdb82	0	1	0	0	1	0	01	11	01	01	
30	6e0f49	02023e	1d6215f	4d9b704	0	0	0	0	0	0	10	10	10	11	
31	5c1e92	04047c	3ac42be	1b36e09	1	0	0	0	0	1	00	01	01	11	1
32	383d25	0808f9	358857d	366dc13	0	1	0	0	0	1	01	10	10	01	0
33	707a4a	1011f3	2b10afa	6cdb827	1	1	1	0	1	0	10	00	01	10	0
34	60f494	2023e6	16215f5	59b704e	1	0	1	0	0	1	11	00	00	01	1
35	41e928	4047cd	2c42beb	336e09d	0	0	1	0	0	1	11	01	00	00	0
36	03d251	808f9a	18857d6	66dc13a	1	0	1	1	0	0	01	11	00	00	0
37	07a4a3	011f34	310afac	4db8274	0	0	0	0	0	1	10	11	01	00	0
38	0f4946	023e69	2215f59	1b704e8	1	1	1	0	1	1	00	11	11	00	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	7f2370	b1552a	1bdb017	0145bfb	1	0	0	0	1	0	01	10	10	00	0
78	7e46e0	62aa54	37b602e	028b7f7	0	0	1	1	1	0	11	00	11	00	0
79	7c8dc1	c554a8	2f6c05c	0516fee	1	1	0	0	0	0	01	10	01	01	1
80	791b83	8aa951	1ed80b8	0a2dfdd	0	0	0	1	1	1	11	00	11	10	0
81	723706	1552a2	3db0170	145bfbb	1	0	0	0	1	0	10	10	01	11	1
82	646e0c	2aa544	3b602e1	28b7f77	1	0	1	1	0	1	01	01	10	11	1
83	48dc18	554a89	36c05c3	516feef	0	1	1	0	0	1	10	10	01	11	0
84	11b830	aa9512	2d80b87	22dfdde	0	0	0	1	0	0	01	00	11	01	0
85	237061	552a24	1b0170e	45bfbbd	0	1	1	0	0	1	10	00	10	11	0
86	46e0c3	aa5449	3602e1c	0b7f77b	0	1	1	0	0	1	01	00	00	11	0
87	0dc186	54a893	2c05c39	16feef6	0	1	1	1	0	1	00	01	00	01	0
88	1b830d	a95126	180b872	2dfddec	1	1	0	0	0	1	00	00	01	00	
K8	**068b482481de44**														

Table A-21. Detailed ReadZ C1-D1 K8

					Taps:		Select:				Shuffle Networks:				
Clock	**LFSR0**	**LFSR1**	**LFSR2**	**LFSR3**	**0**	**2**	**0**	**1**	**2**	**3**	**0**	**1**	**2**	**3**	**O**
Load	282203	23c3bc	018c124	06f1169	1	0	0	1	0	1	01	01	01	01	
1	504407	478778	0318249	0de22d2	0	1	1	1	1	1	11	00	11	00	
2	20880f	8f0ef1	0630492	1bc45a5	0	1	0	0	1	0	01	10	01	10	
3	41101e	1e1de2	0c60925	3788b4b	1	1	0	0	0	0	10	00	10	01	
4	02203d	3c3bc5	18c124b	6f11697	1	1	0	0	0	0	01	01	00	11	
5	04407b	78778a	3182496	5e22d2e	0	0	1	0	0	1	11	10	00	10	
6	0880f7	f0ef15	230492c	3c45a5c	0	0	0	1	0	0	01	01	01	01	
7	1101ef	e1de2a	0609259	788b4b8	1	0	0	1	0	0	10	00	11	10	
8	2203de	c3bc54	0c124b3	7116970	0	0	0	1	1	0	01	10	10	01	
9	4407bd	8778a8	1824966	622d2e1	1	1	0	0	0	1	10	01	01	10	
10	080f7b	0ef151	30492cd	445a5c3	1	0	0	1	0	0	01	11	10	01	
11	101ef6	1de2a3	209259a	08b4b87	0	1	0	1	1	1	11	01	01	11	
12	203dec	3bc547	0124b34	116970f	1	0	0	1	0	1	10	10	10	11	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	7672b0	a3eff4	19a51a4	387be3e	1	0	1	1	0	1	10	10	00	11	
28	6ce560	47dfe9	334a349	70f7c7d	0	1	1	1	0	1	11	01	00	01	
29	59cac1	8fbfd3	2694693	61ef8fb	0	0	1	1	1	1	01	10	01	00	
30	339582	1f7fa7	0d28d26	43df1f6	0	1	0	0	0	0	00	11	00	10	
31	672b04	3eff4e	1a51a4d	07be3ed	1	1	0	1	1	1	00	10	01	00	1
32	4e5609	7dfe9d	34a349b	0f7c7db	0	0	1	1	0	1	01	01	00	10	0
33	1cac12	fbfd3b	2946936	1ef8fb6	0	0	0	1	0	1	00	10	01	01	1
34	395825	f7fa76	128d26d	3df1f6d	1	1	1	1	0	1	00	01	10	00	1
35	72b04b	eff4ec	251a4db	7be3eda	1	0	0	1	1	1	10	00	01	10	0
36	656096	dfe9d8	0a349b7	77c7db5	0	1	1	1	1	0	01	10	00	11	0
37	4ac12d	bfd3b1	146936e	6f8fb6a	1	1	1	1	0	0	00	11	00	10	0
38	15825b	7fa762	28d26dc	5f1f6d4	0	0	0	1	1	0	10	01	01	00	0
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
85	4e7eeb	7ffa3f	365318c	01ba4de	0	0	1	1	1	1	10	11	10	11	1
86	1cfdd6	fff47e	2ca6319	03749bd	1	0	1	1	0	1	01	01	11	01	1
87	39fbac	ffe8fd	194c632	06e937b	1	1	1	1	0	1	10	10	11	10	1
88	73f759	ffd1fb	3298c65	0dd26f7	1	1	1	1	1	0	11	01	10	11	0
89	67eeb3	ffa3f6	25318ca	1ba4dee	1	1	1	1	1	1	11	10	11	10	1
90	4fdd66	ff47ec	0a63195	3749bdd	1	0	1	0	0	0	11	11	01	11	1
91	1fbacc	fe8fd9	14c632a	6e937bb	0	0	0	1	0	0	11	11	11	10	1
92	3f7599	fd1fb3	298c654	5d26f77	1	1	1	0	0	1	10	11	11	01	0
93	7eeb32	fa3f67	1318ca8	3a4deef	0	0	1	0	1	0	11	10	11	10	1
94	7dd664	f47ece	2631950	749bddf	1	0	1	0	1	0	01	01	11	01	0
95	7bacc8	e8fd9d	0c632a0	6937bbe	1	1	0	1	0	1	10	11	01	11	0
96	775990	d1fb3a	18c6541	526f77c	1	1	1	1	0	1	01	11	11	01	
Z	**2efae880e1575606**														

Table A-22. Detailed ReadZ C1-D1 Z

This page is intentionally left blank.

ISBN 0-9675129-8-0

Upstream Link for High-bandwith Digital Content Protection System Revision 1.0 Erratum

Revision 9 April 2001

Notice

This document is an erratum for the previously-published specification:

Upstream Link for High-bandwidth Digital Content Protection, Revision 1.0, Intel Corporation, March 1, 2001

On page 11, the description of An in Table 5-1 has been changed as highlighted below:

Link encryption session random number. This multi-byte value is copied to the video receiver by the graphics driver.

Note: Reading the least significant byte of An may force a return to State A0 (Figure 2-4 of the HDCP specification[3]). The byte read is the least significant byte of the new An.

On page 21, Table A-4 has been changed as highlighted below:

	C1 – D1	C2 – D2	C2 – D1	C2 – D2
status	6105	6115	6008	6007
Cn	2c72677f652c2f27	f0fa8bc54b981cca	bd4bac10c902d2bd	f24977262e7ed2fe
Bksv	e72697f401	511ef21acd	511ef21acd	e72697f401
An	34271c130c	445e62a53a	83bec2bb01	0351f71754
Cs	0000420001	0000430003	0000840005	b500820003
Ku	a25321f0ee8d21	2232a75b461f46	b92f225bfa01d7	d04b7ae589bc76
K1	eb09adb5f6dc25	c424fbf6db045c	623e7c0e7fb070	6619ae14c42333
K2	71ebb3cc7693d4	423ba5fd5fecf0	ecebd28a716c30	130412205bb0b6
K3	fd27048ba34cc4	790514885ea2dd	f9af695ad7dae9	33f4b64a511034
K4	3caf817d0fab9f	8986a731ba0bb4	5f48ccc032937c	2c46bdc08a995f
Kp	98598cc0b4d15a	518b4723c1411f	5603ac3951cc81	e2f24941ac9ad8

Table A-4. ReadStatus With Connection State

On page 29, Table A-14 has been changed as highlighted below:

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	31ccc4	3cac8d	165b048	3043f49	1	0	1	1	1	0	01	01	01	01	
1	639988	795d1b	2cb6091	6087c93	1	1	0	0	1	0	10	10	10	11	
2	473310	f2ba37	196c123	410fd27	0	1	0	1	0	0	01	01	11	10	
3	0c6620	e5746f	32d8246	021fa4f	0	0	1	0	1	0	10	00	11	01	
4	1ccc40	cac8df	25b048d	043f49e	1	0	1	1	1	1	01	00	01	11	
5	399881	95d1bc	0b6091a	087c93d	0	1	0	1	0	1	10	10	00	11	
6	733103	2ba37c	16c1234	10fd27a	0	1	0	1	0	1	00	11	00	01	
7	666206	5746f8	2d82469	21fa4f4	1	0	1	0	0	1	00	01	01	00	
8	4cc40d	ac8df0	1b048d2	43f49c9	0	1	1	1	0	1	10	10	10	00	
9	19881b	5d1bc1	36091a5	07c93d2	1	1	0	0	0	1	01	01	00	10	
10	331037	ba37c3	2c1234b	0fd27a5	1	0	0	0	1	0	11	10	00	01	
11	66206f	746f86	1824696	1fa4f4a	0	1	0	0	0	1	11	01	10	10	
12	4c40dc	e8df0d	3048d2d	3f49c94	0	1	1	1	0	0	10	11	00	11	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	6f0355	869c73	296877b	74a0089	1	0	0	1	0	1	10	11	10	11	
28	5c06ab	0d3cc6	12d0cf6	6940112	1	0	0	0	1	0	01	11	01	11	
29	3c0d57	1a79cc	25a1dcc	5280225	0	0	0	0	0	0	11	10	10	11	
30	781aaf	34f398	0b43bd9	250044b	1	1	0	1	0	0	10	01	01	11	
31	70355c	69c731	16877b2	4a00897	1	0	0	1	0	0	01	10	11	10	1
32	606abc	d3cc62	2d0cf65	140112f	1	1	1	1	0	0	11	01	10	01	1
33	40d579	a79cc5	1a1dcca	280225f	1	0	1	1	1	0	11	10	01	11	1
34	01aaf2	4f398b	343bd95	50044bf	1	0	0	0	1	0	11	11	00	11	1
35	0355e5	9c7316	2877b2b	200897e	1	0	1	0	1	0	11	11	10	10	1
36	06abca	3cc62d	10cf656	40112fc	1	1	0	1	0	0	11	11	11	00	1
37	0d5795	79cc5b	21dccac	00225f8	0	1	1	1	1	1	11	11	11	01	0
38	1aaf2a	f398b6	03bd958	0044bf1	1	1	0	1	1	0	01	11	11	10	0
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	053515	3c8c7c	275bb51	2fdc233	1	1	0	1	1	0	01	00	11	00	1
78	0a6a2b	7d18f9	0cb76a3	5fb8467	1	1	1	0	1	1	11	00	01	01	0
79	14d457	fa31f2	1d6cd46	3f708ce	0	1	1	0	0	1	11	01	00	10	1
80	29a8af	f463c5	3adda8c	7ec119c	1	1	0	0	1	1	01	11	00	01	0
81	53515e	e8c7cb	35bb518	7dc2338	1	0	1	1	1	0	11	10	10	00	0
82	26a2bc	d18f97	2b76a31	7b84671	0	1	0	1	1	0	11	11	01	00	1
83	4d4578	a31f2f	16cd462	7708ce3	0	1	1	0	0	0	10	11	10	01	1
84	1a8af0	463c5f	2dda8c5	6c119c7	0	0	0	0	1	0	01	10	01	11	1
85	3515c0	8c7cbc	1bb518a	5c2338f	0	0	0	0	1	1	10	00	10	11	1
86	6a2bc0	18f97c	376a315	384671e	1	0	0	1	0	0	00	01	01	01	0
87	545780	31f2f9	2ed462b	708ce3d	0	1	1	1	1	0	01	00	11	10	0
88	28af00	63c5f2	1da8c57	6119c7b	1	1	0	1	0	0	00	10	01	01	
K4	3caf817d0fab9f														

Table A-14. Detailed ReadStatus C1-D1 With Connection State K4

On page 30, Table A-15 has been changed as highlighted below:

Clock	LFSR0	LFSR1	LFSR2	LFSR3	Taps: 0	Taps: 2	Select: 0	Select: 1	Select: 2	Select: 3	Shuffle Networks: 0	Shuffle Networks: 1	Shuffle Networks: 2	Shuffle Networks: 3	O
Load	086b9f	00343e	0287817	0000f2b	0	0	1	0	0	0	01	01	01	01	
1	10d73f	00687d	050f02e	0001e56	0	0	1	0	0	0	00	11	10	10	
2	21ae7f	00d0fa	0a1e05c	0003cad	1	0	0	1	1	0	00	10	01	01	
3	435cff	01a1f5	143c0b9	000795a	1	1	1	1	1	0	01	01	00	11	
4	06b9ff	0343ea	2878172	000f2b5	1	1	0	0	1	0	10	10	10	10	
5	0d73fc	0687d5	10f02e4	001e56a	1	0	1	1	1	0	01	01	11	00	
6	1ae7fd	0d0fab	21e05c8	003cad5	1	1	1	0	0	1	10	10	11	01	
7	35cffa	1a1f57	03c0b91	00795aa	1	0	1	0	0	1	11	00	11	10	
8	6b9ff4	343eac	0781722	00f2b55	0	1	0	0	0	1	11	01	10	11	
9	573fc8	687d5d	0f02e45	01e56ab	1	1	0	0	0	1	10	11	00	11	
10	2e7fd0	d0faba	1e05c8a	03cad57	1	1	1	1	0	0	01	11	01	01	
11	5cffa1	a1f574	3c0b914	0795aaf	0	1	1	1	0	0	10	11	11	10	
12	39ff42	43eac9	3817229	0f2b55c	0	1	1	1	1	1	01	01	11	01	
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
27	2127bb	74b298	114a8d2	2af6bc3	1	0	0	1	0	1	00	10	01	11	
28	424f76	c96531	22951a4	55cd7c7	0	0	1	0	1	1	01	01	10	01	
29	049ecc	d2ca62	052a349	2bdaf8c	1	1	0	1	0	0	00	11	01	00	
30	093dd9	a594c5	0a54692	57b5f1c	1	0	0	1	1	1	01	01	11	00	
31	127bb3	4b298a	14a8d24	2f6bc38	1	0	1	0	0	1	11	00	11	10	0
32	24f767	965314	2951a49	5cd7c71	0	1	1	0	1	0	11	01	10	11	0
33	49eecf	2ca628	12a3492	3daf8e2	1	1	1	1	0	1	01	11	01	10	1
34	13dd9e	594c50	2546924	7b5f1c4	1	0	1	0	0	0	10	11	11	01	0
35	27bb3d	b298a0	0a8d248	76bc388	0	0	0	1	0	1	11	10	11	11	1
36	4f767a	653141	151a491	6d7c711	1	0	1	0	1	1	10	11	10	11	1
37	1eecf5	ca6282	2a34922	5af8e22	1	1	1	0	1	1	11	10	11	01	0
38	3dd9ea	94c504	1469244	35f1c45	1	1	1	1	0	1	11	01	11	10	1
...	...	...	...	...	..	..	..	..	..	..	..	..	..	..	..
77	34a73a	708565	323d018	2e5745f	0	1	0	1	1	0	00	10	01	11	0
78	694c75	e10aca	247a031	5cae8bf	1	0	1	0	1	1	00	01	00	11	1
79	529cea	c21595	08f4063	395d17f	1	0	0	0	1	0	10	10	00	01	0
80	2539d4	842b2a	11e80c6	72ba2fe	1	0	0	0	0	1	01	01	10	10	0
81	4a73a8	085655	23d018c	65745fd	1	1	1	0	1	1	11	10	00	11	0
82	14c750	10acaa	07a0318	4ae8bfa	1	1	1	1	0	1	11	01	10	01	0
83	29cea0	215954	0f40630	15d17f5	0	0	1	0	0	0	11	10	01	10	1
84	539d40	42b2a9	1e80c61	2ba2fea	0	1	0	1	0	1	01	01	11	00	1
85	273a80	856553	3d018c2	5745fd5	0	1	0	0	0	0	10	00	11	10	0
86	4e7501	0acaa7	3a03184	2e8bfaa	1	0	1	1	0	0	00	01	10	01	0
87	1cea03	15954e	3406308	5d17f55	0	0	1	1	0	0	10	00	01	11	1
88	39d407	2b2a9c	280c611	3a2feab	1	1	1	0	0	1	01	00	10	10	
Kp	98598cc0b4d15a														

Table A-15. Detailed ReadStatus C1-D1 With Connection State Kp